(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 058 254 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
**07.07.2004 Bulletin 2004/28**

(51) Int Cl.[7]: **G11B 20/00**, G11B 7/007, G11B 23/28, G06F 1/00

(21) Application number: **00108910.1**

(22) Date of filing: **27.04.2000**

(54) **Optical disk, optical disk recording and reproducing apparatus, and method for recording and reproducing**

Optische Platte, optisches Plattenaufzeichnungs- und wiedergabegerät, und Verfahren zur Aufzeichnung und Wiedergabe

Disque optique, appareil pour l'enregistrement et la reproduction de disque optique, et méthode d'enregistrement et de reproduction

(84) Designated Contracting States:
**DE FR GB**

(30) Priority: **28.04.1999 JP 12210499**
**10.05.1999 JP 12819799**
**21.10.1999 JP 29963599**

(43) Date of publication of application:
**06.12.2000 Bulletin 2000/49**

(60) Divisional application:
**04004964.5**

(73) Proprietor: **Matsushita Electric Industrial Co., Ltd.**
**Kadoma-shi, Osaka 571-8501 (JP)**

(72) Inventors:
- **Nagai, Takahiro, Mezon Higashinoda-cho 301**
  **Osaka-shi, Osaka 534-0024 (JP)**
- **Ishihara, Hideshi**
  **Katano-shi, Osaka 576-0054 (JP)**
- **Takagi, Yuji**
  **Hirakata-shi, Osaka 573-0065 (JP)**
- **Yumiba, Takashi**
  **Uji-shi, Kyoto 611-0002 (JP)**
- **Shoji, Mamoru**
  **Sakai-shi, Osaka 591-8032 (JP)**
- **Oshima, Mitsuaki**
  **Kyoto-shi, Kyoto 615-8074 (JP)**
- **Ohara, Shunji**
  **Higashiosaka-shi, Osaka 578-0963 (JP)**
- **Ito, Motoshi**
  **Osaka-shi, Osaka 536-0001 (JP)**
- **Ishida, Takashi**
  **Yawata-shi, Kyoto 614-8331 (JP)**
- **Nakamura, Atsushi**
  **Kadoma-shi, Osaka 571-0064 (JP)**
- **Tadashi, Jahana**
  **Yokohama-shi, Kanagawa 226-0003 (JP)**
- **Nakata, Kouhei**
  **Kawanishi-shi, Hyogo 66-0003 (JP)**

(74) Representative: **Eisenführ, Speiser & Partner**
**Patentanwälte Rechtsanwälte**
**Postfach 10 60 78**
**28060 Bremen (DE)**

(56) References cited:

| | |
|---|---|
| EP-A- 0 442 566 | EP-A- 0 802 527 |
| EP-A- 0 954 173 | EP-A- 0 984 346 |
| WO-A-00/21087 | WO-A-98/58368 |
| GB-A- 2 332 977 | US-A- 5 513 169 |
| US-A- 5 596 639 | US-A- 5 646 993 |
| US-A- 5 745 568 | US-A- 5 752 009 |

- **PATENT ABSTRACTS OF JAPAN vol. 1997, no. 10, 31 October 1997 (1997-10-31) & JP 09 171619 A (SONY CORP), 30 June 1997 (1997-06-30)**
- **PATENT ABSTRACTS OF JAPAN vol. 2000, no. 07, 29 September 2000 (2000-09-29) & JP 2000 113586 A (VICTOR CO OF JAPAN LTD), 21 April 2000 (2000-04-21)**



EP 1 058 254 B1

Printed by Jouve, 75001 PARIS (FR)

## Description

### BACKGROUND OF THE INVENTION

### 1. FIELD OF THE INVENTION

**[0001]** The present invention relates to an optical disk, an optical disk recording and reproducing apparatus, a method for recording, reproducing and deleting data on an optical disk, and an information processing system. In particular, the present invention relates to an optical disk, an optical disk recording and reproducing apparatus, a method for recording, reproducing and deleting data on an optical disk, and an information processing system, which can prevent unjust digital copying from being performed from an optical disk, on which data such as AV data (Audio and Visual Data) including image data of movies and audio data of music protected with copyright is recorded, to the other recording media such as an optical disk of another recording type or the like.

### 2. DESCRIPTION OF THE RELATED ART

**[0002]** An optical disk is superior in random accessibility to conventional tape media, and has such an advantage that deterioration due to repetitive use is reduced because of being capable of non-contacting recording and reproducing using laser light. Further, the optical disk has such an advantage that mass reproduction can be made at low cost by mastering performed by disk manufacturers, and a CD (Compact Disk) becomes generalized as a high quality digital audio instead of a conventional phonograph record for analog recording. Furthermore, recently, a DVD where high quality image data has been digitally recorded (Digital Video Disk or Digital Versatile Disk) is commercialized, and the optical disk will be expected to be further developed as a digital recording medium for AV data in the near future.

**[0003]** On the other hand, in addition to a read-only optical disk on which data has been previously recorded in a pre-pit form by a disk manufacturer, such as a music CD, CD-ROM, DVD-ROM or the like, an optical disk of recording type on which user can record AV data at home, such as CD-R, CD-RW, MO, MD, DVD-RAM or the like has been recently developed and widely spread.

**[0004]** Also, in television broadcasts, digital systems for allowing multi-channeling or various services have been introduced instead of conventional analog systems, and such a trend will be widely spread in the near future. In particular, the optical disk of recording type is expected to be utilized, as recording media of content delivered through digitized broadcasting or communication, for recording AV data mainly for the purpose of time shift utilization where, after contents are accumulated upon being delivered, program selection is performed and the selected content is listened or watched.

**[0005]** Conventionally, an optical disk of recording type which has been utilized mainly for computers is utilized for storing data which has been created by a user himself, and the optical disk of recording type does not have any means for preventing copying from being performed between optical disk of recording types. When the optical disk of recording type is widely utilized, an ordinary user copies recorded data of an optical disk to another optical disk of recording type irregularly as it is so that it becomes possible to obtain unjust reproduction without paying copyright royalty to be paid to an author or writer of this AV data and without deterioration in sound quality and image quality owing to that the optical disk of recording type is digitally recordable, which becomes a factor of preventing spread of excellent content. Regarding an MD on which music or the like is digitally recorded, means for performing generation management for limiting the number of recordings has been introduced, where data together with generation management data is recorded on an optical disk and the number of copyings is limited by the generation management data.

**[0006]** Also, in order to prevent unjust copying of a CD-ROM or a DVD-ROM, for example, a method for forming a Burst Cutting Area (referred to as a BCA hereinafter) which is a write once area for overwriting barcode on a pit section of an optical disk, and for recording IDs on the BCA which are different from each other for each optical disk upon manufacturing optical disks, has been proposed in an international application of International Publication No. WO 97/14144. According to this method, since a password is different for each disk ID, one password can decrypt only a cipher of one disk, so that, even when content is copied unjustly, the content can not be decrypted due to lack of information of a disk ID.

**[0007]** Fig. 39 is a block diagram showing a configuration of a user data area of a conventional DVD-ROM, and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data in the user data area. In the DVD-ROM, as shown in Fig. 39, encryption is performed on content data recorded on a disk.

**[0008]** Referring to Fig. 39, the user data area of the DVD-ROM is constituted by a sector header area 3201, a main data area 3202, and an error detection code 3203. In this case, a sector address 3204 indicating a position of a sector, copyright control information 3205 on which the copyright control information regarding data recorded on the main data area 3202 (for example, a scramble flag, copy control information and the like) is recorded, and a decipher key 3206 for decrypting a cipher when the cipher is performed on data recorded on the main data area 3202 are recorded on the sector header area 3201. Also, mainly AV data required for copyright protection and the like are encrypted and recorded on the main data area 3202.

**[0009]** At the time of reproducing such a user data area, a decipher key 3206 required for reproducing en-

crypted content from the sector header area 3201 is first acquired. The acquired decipher key 3206 is inputted to a key decrypting device 3207, which decrypts the input decipher key 3206 to a content decipher key by using a predetermined disk key, and outputs the content decipher key to a decrypting device 3208. Next, the decrypting device 3208 decrypts the encrypted content of the main data area 3202 using the decrypted content decipher key, according to the copyright control information 3205 which has been stored on the sector header area 3201 corresponding to the main data area 3202, and then, the decrypted content which is reproducible data can be obtained.

**[0010]** In the optical disk according to the configuration shown in Fig. 39, it is possible to perform reading-out from the main data area 3202 through a driving apparatus of a personal computer or the like. However, unjust reproduction or production of pirated version can be prevented by constituting the optical disk so that an area where the decipher key 3206 is recorded can be read out only by an optical disk reproducing apparatus with a regular authentication function.

**[0011]** However, for the unjust copying preventing method using the generation management data, it is inevitable to change the generation management data upon copying (change from "once copying possible" to "copying impossible"). On the other hand, there is such a problem that unjust copying can not be prevented sufficiently by copying data on the optical disk together with the generation management data without changing the generation management data or by altering the generation management data by a computer or the like and recording them on the optical disk. Furthermore, since the number of copyings is limited based on the generation management data which has been previously recorded together with the content, there is such a problem that, even when a regular copyright royalty is paid, data which has been made "copying impossible" is not allowed to be copied to another optical disk at all, and a user must wait for providing content data from a content provider. Both the problems are caused due to that the content provider can not manage content copying onto an optical disk of recording type performed by a user sufficiently.

**[0012]** Recently, personal computers are further improved in performance and further they are connected to networks, so that cipher decryption can be performed at high speed by a plurality of personal computers. In order to further increase robustness of the cipher against such a decryption, it becomes necessary to extend a key length of a key used for the cipher. However, in a key management method for recording a decipher key in a sector header as proposed conventionally, there is such an problem that only a decipher key with a size of a predetermined length (a size of decipher key area) or less is recorded, and a key length can not be elongated for the purpose of improving robustness of a cipher in the future.

**[0013]** EP 0 802 527 A1 discloses an optical disc, an optical recorder, an optical reproducing device, an encrypted communication system and an authorizing system for use of program. Optical discs described therein have auxiliary data recording areas, where different IDs for individual discs, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoder keys when receiving the ciphers, user authorization procedures are simplified.

## SUMMARY OF THE INVENTION

**[0014]** The first object of the present invention is to provide an optical disk, an optical disk recording apparatus, an optical disk reproducing apparatus, an optical disk recording and reproducing apparatus, a method for recording and reproducing data on an optical disk, a method for recording data on an optical disk, a method for reproducing data on an optical disk, a method for deleting data on an optical disk, and an information processing system, which can prevent unjust digital copying which a content provider can not manage.

**[0015]** Also, the second object of the present invention is to provide an optical disk, an optical disk recording apparatus, an optical disk reproducing apparatus, an optical disk recording and reproducing apparatus, a method for recording and reproducing on an optical disk, a method for recording on an optical disk, a method for reproducing on an optical disk, a method for deleting data on an optical disk, and an information processing system, which can enhance reliability of a decipher key required to decrypt data required for copyright protection.

**[0016]** Furthermore, the third object of the present invention is to provide an optical disk, an optical disk recording apparatus, an optical disk reproducing apparatus, an optical disk recording and reproducing apparatus, a method for recording and reproducing data on an optical disk, a method for recording data on an optical disk, a method for reproducing data on an optical disk, a method for deleting data on an optical disk, and an information processing system, which can set robustness level of cipher according to a level of copyright protection of content to be recorded.

**[0017]** In order to achieve the aforementioned objects, an optical disc as claimed in claim 1, an optical disc recording apparatus as claimed in claim 5, an optical disc recording method as claimed in claim 9, an optical disc reproducing apparatus as claimed in claim 13 and an optical disc reproducing method as claimed in claim 16 are proposed according to the present invention.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0018]** These and other objects and features of the present invention will become clear from the following

description taken in conjunction with the preferred embodiments thereof with reference to the accompanying drawings throughout which like parts are designated by like reference numerals, and in which:

Fig. 1 is a plan view illustrating a data recording area of the optical disk of recording type 100 of a first preferred embodiment according to the present invention;

Fig. 2A shows a block diagram and a cross section view illustrating an apparatus configuration for forming the BCA 106 of the optical disk 100 shown in Fig. 1;

Fig. 2B shows a cross section view of the optical disk 100 after formation of the BCA 106 of the optical disk 100 shown in Fig. 1 and a graph showing a strength of a reflected light in the horizontal direction;

Fig. 3 is a diagram showing a recording format of the BCA 106 shown in Fig. 1;

Fig. 4 shows a view for illustrating a sector structure of sector data 401 within a user data area 102 shown in Fig. 1;

Fig. 5 shows a view illustrating a configuration of a key management information area 107 shown in Fig. 1;

Fig. 6A is a block diagram showing a recording method for recording a descramble key and AV data in the sector data 401 shown in Fig. 1 according to a modified preferred embodiment of the first preferred embodiment;

Fig. 6B is a block diagram showing a recording method for recording a key index to the descramble key and the AV data into the sector data 401 shown in Fig. 1, according to the first preferred embodiment;

Fig. 7 is a block diagram showing a configuration of an optical disk recording and reproducing apparatus of a second preferred embodiment according to the present invention;

Fig. 8 is a flowchart showing a recording process of AV data carried out by a control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7;

Fig. 9 is a flowchart showing an allocating process of a key management information area carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7;

Fig. 10 is a flowchart showing a recording process of a descramble key carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7;

Fig. 11 is a flowchart showing a reproducing process of AV data carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7;

Fig. 12 is a flowchart showing an acquiring process of a descramble key carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7;

Fig. 13 is a block diagram showing a method for determining whether or not a descramble key is regular based on an encrypted descramble key according to a modified preferred embodiment of the first preferred embodiment;

Fig. 14 is a view showing a configuration of the descramble area management table according to a modified preferred embodiment of the first preferred embodiment;

Fig. 15A is a diagram showing whether or not copying or reproducing of contents is possible within the same region or in different regions in the case that a region identifier is recorded when a content is recorded in the first preferred embodiment;

Fig. 15B is a diagram showing whether or not copying or reproducing of the content is possible in the same region or in different regions in the case that a region identifier is previously recorded when an optical disk is shipped in the first preferred embodiment;

Fig. 16 is a plan view showing a data recording area of an optical disk 1101 of a third preferred embodiment according to the present invention;

Fig. 17 is a waveform diagram showing signal waveforms of a reproduced signal 1201 and a reproduced binarized signal 1207 in a BCA reproducing circuit 1401 according to the third preferred embodiment;

Fig. 18 is a block diagram showing a configuration of the BCA reproducing circuit 1401 according to the third preferred embodiment;

Fig. 19 is a block diagram showing a configuration of an optical disk recording and reproducing system according to the third preferred embodiment;

Fig. 20 is a block diagram showing a configuration of an optical disk recording and reproducing system of the fourth preferred embodiment according to the present invention;

Fig. 21 is a plan view showing a data recording area of an optical disk 1601 of a fifth preferred embodiment according to the present invention;

Fig. 22 is a block diagram showing a configuration of an optical disk recording and reproducing system according to the fifth preferred embodiment;

Fig. 23 is a table showing a configuration of an ID adding table according to the fifth preferred embodiment;

Fig. 24 is a plan view showing a data recording area of an optical disk 1101a according to a modified preferred embodiment of the third preferred embodiment;

Fig. 25 is a plan view showing a data recording area of an optical disk 1601a according to a modified preferred embodiment of the fifth preferred embodiment;

Fig. 26 is a block diagram showing a configuration

of a user data area on the optical disk, and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data in a user data area, according to a sixth preferred embodiment of the present invention;

Fig. 27 is a block diagram showing an arrangement of copyright control information and decipher key into a user data area, and an arrangement of an encrypted content into a main data area, in the optical disk according to the sixth preferred embodiment;

Fig. 28 is a block diagram showing an arrangement of the case where a unit for error correction is applied for a plurality of sectors in the optical disk according to the sixth preferred embodiment;

Fig. 29 is a block diagram showing a configuration of a lead-in area 2401 and a user data area 2402 within an optical disk of a seventh preferred embodiment according to the present invention, and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data stored in the lead-in area 2401 and the user data area 2402;

Fig. 30A is a block diagram showing a data configuration in the case of indicating an unrecorded status by an initial value of a decipher key in the main data area of the lead-in area within the optical disk according to the seventh preferred embodiment;

Fig. 30B is a block diagram showing a data configuration in the case of indicating a recorded status by a decipher key status table in the main data area of the lead-in area within the optical disk according to the seventh preferred embodiment;

Fig. 31 is a block diagram showing an arrangement of a decipher key in the optical disk according to the seventh preferred embodiment;

Fig. 32 is a block diagram showing a data configuration for managing data of an optical disk by a file management system of an eighth preferred embodiment according to the present invention;

Fig. 33 is a flowchart showing a recording process of content required for copyright protection, which is carried out by the file management system according to the eighth preferred embodiment;

Fig. 34 is a flowchart showing a reproducing process of content, which is carried out by the file management system according to the eighth preferred embodiment;

Fig. 35 is a flowchart showing a deleting process of content, which is carried out by the file management system according to the eighth preferred embodiment;

Fig. 36 is a block diagram showing a configuration of an optical disk system of a ninth preferred embodiment according to the present invention;

Fig. 37 is a block diagram showing a configuration of a user data area within an optical disk of a tenth preferred embodiment according to the present invention, a configuration of an optical disk recording apparatus for encrypting and recording a content into the user data area, and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data stored in the user data area;

Fig. 38 is a block diagram showing a configuration of a user data area within an optical disk of an eleventh preferred embodiment according to the present invention, a configuration of an optical disk recording apparatus for encrypting and recording a content into the user data area, and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data of the user data area; and

Fig. 39 is a block diagram showing a configuration of a user data area of a DVD-ROM, and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data of the user data area according to a prior art.

## DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

**[0019]** Preferred embodiments according to the present invention will be described below with reference to the attached drawings.

## FIRST PREFERRED EMBODIMENT

**[0020]** Fig. 1 shows a plan view illustrating a data recording area of an optical disk 100 of recording type of the first preferred embodiment according to the present invention. This optical disk 100 of recording type is a recording medium which is capable of recording digital data, and includes a write-once type non-rewritable optical disk and a rewritable optical disk.

**[0021]** Referring to Fig. 1, 101 denotes a lead-in area for recording therein management information for the optical disk 100, and 102 denotes a user data area for recording therein digital data which needs copyright protection, such as (a) AV data content including at least one of image data (including still picture images and animated picture images) such as movies or the like, and speech sound data such as music or the like; and (b) computer software. 103 denotes a lead-out area for recording therein defect management information or the like. The lead-in area 101 is constituted by a read-only area 104 in which data is recorded in a form of pre-pits, and a recording and reproducing area 105 which is a rewritable area with guide grooves. In this case, in the read-only area 104, a control area or the like which describes physical characteristics of the optical disk 100 is recorded in a form of pre-pits by the manufacturer. In the lead-out area 103 and rewritable area 105, data for writing test performed by an optical disk recording apparatus, management information for managing defects on the optical disk 100 are recorded by an optical disk recording apparatus. In addition, on the inner peripheral

side of the read-only area 104 in the lead-in area 101, a BCA 106 formed as disk individual information is once written on the optical disk 100 by the following well known method, after completion of the optical disk 100 on which content has been recorded.

**[0022]** Fig. 2A shows a block diagram and a cross sectional view illustrating an apparatus configuration when forming the BCA 106 of the optical disk 100 shown in Fig. 1, and Fig. 2B shows a cross sectional view of the optical disk 100 and a graph showing an intensity of reflected light in the horizontal direction after formation of BCA 106 of the optical disk 100 shown in Fig. 1.

**[0023]** Referring to Figs. 2A and 2B, an example of the optical disk 100 of double-side recording type is shown, and the optical disk 100 is constituted so that a recording layer 202, a reflecting layer 203, a bonding layer 204, a reflecting layer 205 and a recording layer 206 are inserted between two substrates 201 and 207.

**[0024]** When the BCA is recorded on the optical disk 100, as shown in Fig. 2A, data after phase encoding modulation in a stripe form is recorded so as to overlap on pits by irradiating a laser beam in a form of pluses from a high power laser light source 211 onto, for example, the reflecting layer 205 of the optical disk 100 through a focusing lens 212 to eliminate or remove a part of the reflecting layer 205. Upon reproducing the signals, as shown in Fig. 2B, the signals, resulting from a lowered amount of reflecting light from the portions where the reflecting layer 205 is eliminated or removed, are intermittently reproduced. The BCA data is reproduced through the phase encoding demodulation after the reproduced signals are binarized. The BCA formed by such a recording system can record a disk identifier which is specific information for each optical disk 100, and further, the BCA has such a feature that it is impossible to falsify recorded data.

**[0025]** Fig. 3 shows a view of a recording format of the BCA 106 shown in Fig. 1. As shown in Fig. 3, in the BCA 106, a synchronization code 301, an error detection code 302, an error correction code 303 and the like are recorded to improve the reading-out factor of the BCA data 304. By connecting the plurality of BCA data 304, a disk identification information 305 is constituted. In the disk identification information 305, there are recorded types of data that are recordable into the user data area and the types of data which are reproducible from the user data area. It is impossible for the data of BCA 106 to falsify, and therefore, this can limit to a certain degree of disk usage, by the user, by means of the disk identification information recorded when the optical disk 100 is manufactured.

**[0026]** Fig. 4 shows a sector structure of sector data 401 within the user data area 102 shown in Fig. 1. Referring to Fig. 4, the user data area 102 shown in Fig. 1 has a sector structure which is accessible by a unit of a certain amount, and the sector data 401 is constituted by a header 402, main data 403 and an error detection code 404.

**[0027]** The main data 403 is an area in which AV data, computer data and the like are recorded. In the header 402, a data ID (data identifier) 405, an ID error detection code 406, scramble control information 407, key information 408 or the like are recorded. In the data ID 405, a logical address for identifying sectors or the like is recorded, and the ID error detection code 406 is provided for detecting errors in the data IDs. The scramble control information 407 is a flag for showing whether or not the main data has been scrambled, and in the key information 408, there is recorded information about a key for descrambling the main data. As the information about the key, the descramble key itself (in the modified preferred embodiment of the modified preferred embodiment of the first preferred embodiment) or a key index (in the first preferred embodiment), which is a pointer to the descramble key recorded onto another area of the optical disk 100, are recorded. An example of Fig. 4 shows the case where a key index is recorded for referring to the descramble key recorded in the key management information area 107 shown in Fig. 1 which is another area of the optical disk 100.

**[0028]** Fig. 5 shows a configuration of the key management information area 107 shown in Fig. 1. Referring to Fig. 5, the key management information area 107 is constituted by a key information area 501, a content information area 502 and a key index list area 503.

**[0029]** In the key information area 501, the number of recorded key areas 504 is recorded, and the key information area 501 includes (a) a descramble key area 505 which is an area for recording the descramble key to descramble the scrambled AV data or the like, and (b) a key status area 506 for recording therein a recording status (indicating unused, area reservation, recorded or the like) of the descramble key recorded in the descramble key area 505. In the descramble key area 505, a plurality of descramble keys are recorded, and a key index for representing the stored position in the descramble key area 505 is recorded in the key index list area 503. The above-mentioned plurality of descramble keys are possible to be referred to by this key index. In the key status area 506, the status information for representing the recording status of the descramble keys is stored at a position which is possible to be referred to by the key index.

**[0030]** In the content information area 502, the contents recorded on the optical disk 100 are registered when copyright protection is necessary, and the information with respect to keys used for that content is registered. In the content information area 502, the number of contents 507 registered in the key index list area 503 and content information 508 for the content number are recorded. In addition, in the content information 508, there are recorded a content ID for identifying the content, the number of descramble keys used for the content, and the pointer to the key index list 509 which records the used keys. The key index list area 503 is an area for recording indexes to refer to the keys used for

the content in a form of in content unit. In the key index list area 503, a key index for referring to the entire recording area of the descramble keys used for the content is recorded.

**[0031]** The optical disk of recording type 100 constituted in this way makes it possible to control the recording operation and the reproducing operation in accordance with the protection level or the usage level of the copyright held by the contents, by recording information for representing conditions or status for disk usage on the disk identification information which is difficult to rewrite such as a region identifier, a data category identifier and a disk identifier upon manufacturing, and by detecting such information by an optical disk and reproducing apparatus. Since data is recorded so as to make it difficult to rewrite so that a user can not change data, even in the case that the copyright protected content is copied to another optical disk, the disk identification information cannot be copied while it remains possible to copy the user data area. Accordingly, by recording the data scrambled using the disk identification information on the optical disk, it can be prevented from reproducing correctly since there exists a user data area which cannot be descrambled in the optical disk having different disk identification information.

**[0032]** Fig. 15A shows a diagram showing whether or not copying or reproducing the content is possible in the same region as well as in a different region in the case that a region identifier is recorded when the content is recorded in the first preferred embodiment, and Fig. 15B shows a diagram indicating whether or not the copying or the reproduction of the content is possible in the same region as well as a different region in the case that a region identifier is recorded in advance when the optical disk is shipped in the first preferred embodiment.

**[0033]** For example, as shown in Fig. 15A, in the case that a region identification code is not recorded when the optical disk is shipped, and the region identifier, for representing the region where the contents are available when the contents are recorded, is recorded in a recording and reproducing area, the usage can be prevented in another region. However, the contents are recordable in a disk (for a region RC2 shown in Fig. 15A) to be used in another region, and it is possible to reproduce the content correctly. A recording medium, in which a digital copying of the content is possible, is provided with a tax imposing system to protect the benefit of copyright holders which collects an added charge when the optical disk is sold. However, the added charge differs according to country and in the case that the recording medium to be used in another country is utilized unjustly the possibility remains that the copyright holders will not be able to share in the appropriate profit.

**[0034]** As shown in Fig. 15B, by recording in advance at the time of shipping in such way that the region identifier cannot be falsified, copying or reproduction of the content to an optical disk to be used in another region can be prevented. In a manner similar to that of above, in the case that a data category identifier is recorded as disk identification information, copying or reproduction of the content to the disk on which the data is recordable and reproducible can be limited by comparison between category identifiers which the record data have. In the case that an inherent disk identifier for each optical disk is recorded as disk identification information, the recorded data can be made available only by the optical disk by encrypting the recorded data with the disk identifier.

**[0035]** In the present preferred embodiment, the data scrambled by the disk identification information may be AV data or computer data which needs copyright protection or may be descramble keys for descrambling scrambled AV data or computer data.

**[0036]** Fig. 13 shows a block diagram showing a method for judging whether or not a descramble key is a regular descramble key based on the encrypted descramble key according to the modified preferred embodiment of the modified preferred embodiment of the first preferred embodiment. As shown in Fig. 13, the data obtained by adding an error detection code for detecting errors in the descramble key to the descramble key may be scrambled using disk identification information to calculate an encrypted descramble key, which may be recorded on the optical disk. In the optical disk reproducing apparatus, the encrypted descramble key is decrypted into a descramble key, and an error detection code so that it is judged whether or not the decrypted descramble key is a regular descramble key by detecting errors based on the parity check in the decrypted error detection code. For example, in the case of descrambling using different disk identification information, an error descramble key is produced so that an irregular copy can be detected by checking the error detection code for determining that it is not any regular descramble key.

**[0037]** As another method for recording disk identification information, by preparing stampers formed with a plurality of types of disk identification information in a form of pre-pits and by forming an optical disk from each of the stampers, different usage limitation may be given to respective optical disks formed from different stampers. In addition, by scrambling the disk identification information using a secret key and by recording the scrambled disk identification information on the optical disk, the protective level of the copyright described in the disk identification information is kept unknown to the users, and as a result, the copyright protection is further enforced.

**[0038]** The case where the descramble key itself is recorded as the information about the key described in Fig. 4 (in the modified preferred embodiment of the first preferred embodiment) and the case where the key index, which is a pointer to the descramble key recorded in another area of the disk, is recorded (in the first preferred embodiment) will be described with reference to Figs. 6A and 6B. Fig. 6A shows a block diagram showing a recording method for recording a descramble key and

AV data in the sector data 401 shown in Fig. 1 according to the modified preferred embodiment of the first preferred embodiment, and Fig. 6B shows a block diagram showing a recording method for recording a key index and AV data to a descramble key in the sector data 401 shown in Fig. 1 according to the first preferred embodiment.

**[0039]** In the case of Fig. 6A, in the same sector data 401, the main data 403 and the descramble key which is key information 408a required for descrambling of the main data 403 are recorded. Thus, it is necessary to acquire a descramble key required for descrambling when AV data are recorded. That is to say, the acquisition or the purchase of the key itself are indispensable or inevitable when AV data are recorded.

**[0040]** On the other hand, in the case of Fig. 6B, in the same sector data 401, the main data 403, and the key index which is the key information 408 for referring to the descramble key area for recording the necessary information for descrambling the main data 403 are recorded, and the descramble key is recorded in an area designated by the key index. When the AV data are recorded, the key ID indicating which key among the keys used in the recorded content can descramble is acquired, and the key information 408 is acquired which is a key index corresponding to the key ID from the key index list included in the content information, which is recorded together with the main data 403. The recording of the descramble key is carried out when the descramble key is obtained to be recorded in the descramble key area shown by the key index corresponding to the key ID. As a result, AV data and the descramble key corresponding to the AV data can be recorded independently. That is to say, the recording of AV data and acquisition or purchase of the key can be carried out independently so that the acquisition or the purchase of the key is not necessarily required when the AV data are recorded. It becomes possible for the user to utilize a method for recording the content and acquiring the key when actually reproducing.

**[0041]** Fig. 14 shows a configuration view of a descramble area management table according to a modified preferred embodiment of the first preferred embodiment. In the above-mentioned preferred embodiments, in order to correlate the encrypted content with the descramble key for descrambling its cipher the cases in which the key index is recorded for referring the descramble key to the same sector data 401 are described, however, the descramble area management table shown in Fig. 14, which manages the corresponding relationships between the address range of the sectors in which the encrypted content is recorded and the descramble key, may be used. This descramble area management table represents the address range of the sector in which the encrypted content is recorded with the starting address and the completion address, and when the data of the sector is reproduced, the descramble key is referred to and then the encrypted content is descrambled.

**[0042]** In order to acquire the recorded content and the descramble key used for the recorded content, the contents ID that makes the content identifiable is utilized. As shown in Fig. 5, in the content information recorded in the content management list within the content information area 502 recorded on the optical disk, the content ID and the list of the descramble key used for the content are recorded. By having a list configuration where a plurality of descramble keys can be used for one piece of content, such services are made available that a part of the content or a part of the software can be sold.

**[0043]** In the modified preferred embodiment mentioned above in reference to Fig. 13, when the data where the descramble key to which the error detection code is added such as a check sum or a cyclic redundancy check code is scrambled in the disk identification information is copied unjustly onto another disk, it can be detected as an error by descrambling with different disk identification information. In such a case, it is also possible to acquire a descramble key that is scrambled by disk identification information recorded on the optical disk, and to form a disk which can reproduced correctly by replacing that descramble key with the acquired descramble key.

**[0044]** The key management information area 107 shown in Fig. 1 is recorded in a lead-in area 101 which is rewritable. Generally, the user data area 102 comprises a user area which is accessible from a drive apparatus of a personal computer, and a spare area for the defect sector on an optical disk, and for the conventional READ command and WRITE command, only the user area can be accessible as a logical continuous area. By placing the key management information in the lead-in area 101, direct access from the drive apparatus of the personal computer or the like can be prevented so that it can be made impossible to acquire a key for descrambling the scrambled AV data or the like from the personal computer.

## SECOND PREFERRED EMBODIMENT

**[0045]** Fig. 7 shows a block diagram illustrating a configuration of an optical disk recording and reproducing apparatus of the second preferred embodiment according to the present invention. This optical disk recording and reproducing apparatus is provided for recording contents of AV data such as image data or music data which require copyright protection for the optical disk 100 according to the first preferred embodiment.

**[0046]** Referring to Fig. 7, 701 denotes an optical disk of the first preferred embodiment, 702 denotes an optical head which is an optical pickup constituted by a semiconductor laser and optical elements, and 703 denotes a recording and reproducing control circuit for controlling the operation of the semiconductor laser and for binarizing the reproduced signals. 704 denotes a modu-

lating and demodulating circuit for digitally modulating digital data to be recorded and digitally demodulating the binarized reproducing signals, and 705 denotes an error detecting and correcting circuit for error detection and correction processing of errors caused by scratches, dust or the like on the optical disk 701 and for performing error correction code generation processing required for the error-detection and correction processing. 706 denotes a buffer memory of a RAM used for a working memory and a data buffer memory of the error detecting and correcting circuit 705, 707 denotes a descramble circuit for descrambling scrambled recorded AV data, and 708 denotes an MPEG decoding circuit for expanding compressed recorded dynamic image data or the like. 709 denotes an output circuit for D/A converting expanded image data to generate and output video signals and audio signals, 710 denotes a control CPU for controlling the entire operation of the optical disk recording and reproducing apparatus, and 711 denotes a communication circuit for acquiring a descramble key for descrambling the cipher placed in the contents. 712 denotes a data receiving circuit for receiving digital data of the encrypted content such as image data and music data from a communication terminal apparatus such as a set-top box.

**[0047]** A data recording operation of the optical disk recording and reproducing apparatus of Fig. 7 constituted as described above will be described. The digital data of the encrypted contents such as image data or music data transmitted form the communication terminal apparatus such as a set-top box or an MPEG encoder are temporarily stored in the buffer memory 706 after being received by the data receiving circuit 712. The error detecting and correcting circuit 705 generates error detection and correction code required for the error detection and correction process caused by scratches or dust on the optical disk 701 in the digital data of the stored contents to reconfigure the record data. For the error detection and correction code, a code such as a well known Reed-Solomon code is used. In this case, the reconstituted record data includes digital data of content and error detection and correction code. The modulating and demodulating circuit 704 uses a modulation system such as an 8/16 modulation system upon recording, and digitally modulates the record data. Also, the recording and reproducing control circuit 703 modulates the intensity of the power of the laser beam outputted from the optical head 702 according to the record data modulated digitally so that the laser is irradiated onto the optical disk 701 to record the record data onto the optical disk 701.

**[0048]** Fig. 8 shows a flowchart indicating an AV data recording process carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7.

**[0049]** Referring to Fig. 8, first of all, in step S801, the disk identification information of the lead-in area 101 is reproduced prior to recording of the AV data from the optical disk 701, then in step S802 it is determined whether or not the digital data of the contents to be recorded at the present are recordable from the type or class of data recordable in the user data area 102 which are recorded in the disk identification information. In the case of YES in step S802, the program flow proceeds to step S803, while in the case of NO, the recording operation is stopped in the step S810, and then the recording process of the AV data is completed.

**[0050]** In step S803, the data of the sector where the key management information is recorded in the lead-in area 101 is reproduced, and in step S804 it is determined whether or not an area is allocated for the key information required for recording the contents in the reproduced key management information. In the case of NO in step S804, after allocating an area for recording the key information in the key management information area 107, the program flow proceeds to step S806. On the other hand, in the case of YES in step S804 the program flow directly proceeds to step S806.

**[0051]** In the case that the content is recorded, the control CPU 710 of the optical disk recording and reproducing apparatus receives the record data of the encrypted content, and information with respect to the descramble key for descrambling the cipher via the data receiving circuit 712, from the communication terminal apparatus. In this case, the information with respect to the key is the key itself used for the contents or a key ID for indicating to which key it corresponds among the keys used in the entire contents. In the case that the key ID is received, in step S806, the received key ID is converted into a key index which is a pointer for indicating an area where a descramble key corresponding to the key ID is recorded, and the converted descramble key is placed in a header area of the sector where the data of the contents to be decrypted with the descramble key is recorded. Then, in step S807, the control CPU 710 carries out the following record data processing by controlling the recording and reproducing control circuit 703, the modulating and demodulating circuit 704 and the error detecting and correcting circuit 705. In this processing, the codes for the error detection and correction is added to the sector data which is desired to be recorded, and then, the sector data with those codes added are digitally modulated by using a modulation system such as a well known 8/16 modulation system so that the optical head 702 is controlled to locate at a predetermined recording position, and the intensity of the laser beam is modulated according to the record data digitally modulated. By doing this, the record data is recorded on the optical disk 701, and in addition, in step S808 it is determined whether or not the recording of the contents has been completed, and in the case of NO, the program flow goes back to step S806 to repeat the above-mentioned processing. In the case of YES in step S808, the updated key management information is recorded in the key management information area 107 on the optical disk 701 in step S809, and then, the recording

process of the AV data is completed.

**[0052]** Fig. 9 shows a flowchart showing an allocating process of the key management information area carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7. This process is provided for allocating areas for recording a descramble key prior to recording data of content.

**[0053]** Referring to Fig. 9, in step S901, for example the information with respect to the key of the content recorded from an electronic program guide or the like (including the number of used descramble keys) is acquired, and then, in step S902, the key management information within the key management information area 107 recorded in the optical disk 701 is reproduced. Then in step S903, empty areas of the descramble key area 505 are searched from the key status area 506 so as to determine whether or not the descramble key used in the content to be recorded can be recorded. In the case of NO in step S903, the recording operation is stopped in step S907, and then, the allocating process is completed. On the other hand, in the case of YES in step S903, the contents to be recorded are registered in the content list within the content information area 502 so that recording areas are allocated by setting area reservation flags in corresponding key status areas in order to reserve an area required for the recording of descramble key in the descramble key area 505 in step S905. In addition, in step S906, a key index indicating allocated areas for recording descramble keys are formed as a key list, and then, after a pointer set as the content information is allocated, the allocation process is completed.

**[0054]** Fig. 10 shows a flowchart showing a recording process of the descramble key carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7. This recording process is provided for recording a descramble key acquired from a key management center in the optical disk 701.

**[0055]** Referring to Fig: 10, first of all, in step S1001, after the disk identification information of the lead-in area 101 on the optical disk 701 is reproduced, the disk identification information and the key ID for identifying keys required for descrambling for the desired content are transmitted to the key management center via the communication circuit 711 in order to acquire a descramble key from the key management center in step S1002. In the key management center, a descramble key required for descrambling of the content from the given key ID are selected so that the descramble key are encrypted using the information, such as the transmitted disk identification information, and then returned.

**[0056]** After the descramble key corresponding to the key ID is acquired via the communication circuit 711 from the key management center in step S1003, the data of the key management information area 107 is reproduced so that the key index for indicating an area for recording the descramble key is acquired from the key index list indicated by key ID among the data within the reproduced key management information area 107 in step S1004. Then in step S1005, the descramble key acquired above is allocated in the descramble key area indicated by the key index, and an acquired flag for indicating a key acquired in the corresponding key status area 506 is set. In addition, in step S1006, whether or not the acquisition of all the keys are completed is determined, and then, in the case of NO the above-mentioned process is repeated by returning to step S1003. On the other hand, in the case of YES in step S1006, the updated key management information is recorded in the key management information area 107 in step S1007, and then, the descramble key recording process is completed.

**[0057]** Next, the data reproducing operation of the optical disk recording and reproducing apparatus of the present embodiment will be described in reference to Fig. 7. The digital data recorded on the optical disk 701 is reproduced as follows. A laser beam from the semiconductor laser from the optical head 702 is irradiated onto the optical disk 701 so that, at that time, the reflected light which is reflected on the optical disk 701 is entered into the recording and reproducing control circuit 703 via the optical head 702. The recording and reproducing control circuit 703 generates and outputs a generated reproduced binarized signal to the modulating and demodulating circuit 704 by carrying out amplification and by a binarizing process after photoelectrically converting the entered reflected light. The modulating and demodulating circuit 704 digitally demodulates the digitally modulated signal into a digital signal by using a modulating system such as a well known 8/16 modulating system upon recording, and then, outputs the resulting digital signal to the error detecting and correcting circuit 705. Then the error detecting and correcting circuit 705 uses the buffer memory 706 as a working memory to carry out detecting and correcting processes of the errors caused by scratches or dust on the optical disk 701. This error detecting and correcting process is carried out by decoding, for example, well known Reed-Solomon code.

**[0058]** The reproduced data which are processed for error detection and correction is outputted to the descramble circuit 707 for carrying out the descramble process. The descramble circuit 707 uses the descramble key of the key management information area 107 reproduced prior to the data reproduction in advance, and performs a descramble process for the reproduced data, which is then outputted to the MPEG decoding circuit 708. Then the MPEG decoding circuit 708 expands the compressed dynamic image data and music data, and then, the expanded data is outputted to the output circuit 709. In addition, the output circuit 709 D/A converts the inputted expanded data into video and audio signals, and outputs the resulting video and audio signals to upper-level apparatuses such as a television set, an audio device or the like.

**[0059]** Fig. 11 shows a flowchart showing a reproduc-

tion process of AV data carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7.

**[0060]** Referring to Fig. 11, first of all, in step S1101, prior to recording of the AV data from the optical disk 701, the disk identification information within the lead-in area 101 is reproduced, and in step S1102, it is determined whether or not the content desired to be reproduced at present is reproducible from the types of reproducible data recorded in the disk identification information. In the case of NO in step S1102, the reproducing operation is stopped in step S1112, and then, the reproducing process of the AV data is completed. On the other hand, in the case of YES in step S1102, the data in the sector where the key management information is recorded within the key management information area 107 of the lead-in area 101 are reproduced, and it is determined whether or not the key information required for the reproduction of the content has been recorded in the key management information reproduced in step S1104. In the case of YES in step S1104, the program flow proceeds to step S1106 directly. On the other hand, in the case of NO in step S1104, in step S1105, a descramble key is acquired via the communication circuit 711 from the key management center which manages the keys, and is recorded in the key management information area 107 on the optical disk 701, then, the program flow proceeds to step S1106.

**[0061]** Then in step S1106, the control CPU 710 makes the optical head 702 move to the user data area of the optical disk 701, and controls the recording and reproducing control circuit 703, the modulating and demodulating circuit 704 and the error detecting and correcting circuit 705 so that the AV data are reproduced. Then in step S1107, the descramble key required for the descrambling of the sector data is acquired from the descramble key area 505 indicated by the key index included in the header of the reproduced sector, and then, in step S1108, the scrambled information for the descramble key is decoded by descrambling by means of the disk identification information. In addition, in step S1108, by checking the error detection code added to the descramble key, it is determined whether or not the descramble key has an error. In the case of YES in step S1108, the contents are judged as obtained irregularly (or the contents are copied irregularly), the reproducing operation is stopped in the step S1112, and then, the reproducing process of the AV data is completed.

**[0062]** On the other hand, in the case of NO in step S1108, the data of the content is descrambled by the descramble key in S1109, and the descrambled AV data is outputted to the MPEG decoding circuit 708 in step S1110. Then the control CPU 710 MPEG-expands the descrambled AV data through a predetermined MPEG system by controlling the MPEG decoding circuit 708 and the output circuit 709, and then, the MPEG-expanded AV data is D/A converted into video signals and audio signals to be outputted to upper-level devices such as a television set, an audio device or the like. Then in step S1111, it is determined whether or not the reproduction of the content is completed, and in the case of NO the program flow returns to step S1106 to repeat the above-mentioned process. On the other hand, in the case of YES in step S1111, the reproducing process of the AV data is completed.

**[0063]** In the case that an error is detected in step S1109, the content is regarded as obtained irregularly, for example, the content is regarded as copied irregularly, the reproducing operation is stopped. However, the key information may be acquired from the key management center which manages the keys via the communication circuit 711 and recorded in the key management information area 107 on the optical disk 701 by carrying out the process of step S1105 in the same way as the case where any key is not recorded. By doing this, even the copied AV data can become reproducible by obtaining the key in a regular procedure.

**[0064]** Fig. 12 shows a flowchart showing an acquiring process of descramble key carried out by the control CPU 710 of the optical disk recording and reproducing apparatus shown in Fig. 7. This process is provided for reproducing descramble keys from the reproduced key index, and this process is carried out prior to the reproducing process of the AV data as shown in Fig. 11.

**[0065]** Referring to Fig. 12, first of all, in step S1201, it is determined whether or not the data in the reproduced sector area is scrambled by the scramble control information, and in the case of NO, the program flow proceeds to step S1206. On the other hand in the case of YES in step S1201, a key index is acquired by reproducing key information recorded in the same sector area as the above-mentioned sector area in step S1202, and then, the descramble key indicated by the above-mentioned key index is acquired from the descramble key area 505 in step S1203, and afterwards in step S1204, the acquired descramble key is descrambled by using the disk identification information, and it is determined whether or not an error exists in the descramble key by checking the error detection code. In the case of YES in step S1204, the reproducing operation is stopped in step S1205, and the acquiring process of the descramble key is completed. On the other hand, in the case of NO in step S1204, the program flow proceeds to step S1206. When the reproduced sector is not scrambled or when any error is not found to exist as a result of descrambling the descramble key by the disk identification information, permission for the reproducing operation is granted in step S1206, the data of the reproduced sector is outputted, and then, the acquired process of the descramble key is completed.

**[0066]** As described above, in the optical disk and in the optical disk recording and reproducing apparatus of the preferred embodiment according to the present invention, the recording and reproducing operations can be controlled by the user by using disk identification information for read-only made at a disk manufacturing

stage. In addition, by scrambling a part of the data using the above-mentioned disk identification information, it can be prevented from reproducing normally data on the disk where the user data area is physically copied. Also, by allocating the descramble key required for the data descrambling in a different area from that for the data, the recording of the content and the recording of the descramble key can be carried out independently. Thus, by recording the contents and by acquiring the descramble key if necessary, for example, when the data of the content are reproduced, the content can be maintained in a reproducible state or status. At this time, by scrambling the descramble key with the disk identification information, an irregular usage through physical copying can be explicitly prevented in the same way as that described above. In addition to this, a disk copied irregularly could become an optical disk which can be reproduced normally by formally acquiring the descramble key scrambled with the disk identification information of the optical disk from the key management center and by recording the acquired descramble key in the optical disk.

**[0067]** Although already encrypted data of the content inputted to the optical disk recording and reproducing apparatus are described above, by providing a circuit for encrypting the content within the optical disk recording and reproducing apparatus, the same effects can be obtained by encrypting the data of the inputted contents and recording that data on the optical disk.

**[0068]** Although in the present preferred embodiment, by encrypting only the descramble key which is required for decrypting the encrypted content using the disk identification information, copying between the disks having different disk identification information is prevented, copying can be prevented by encrypting the content itself using the disk identification information. In addition, by encrypting the disk identification information using a secret key, it becomes possible to make the irregular decrypting of the content recorded on the disk more difficult.

## ADVANTAGEOUS EFFECTS OF FIRST AND SECOND PREFERRED EMBODIMENTS

**[0069]** An optical disk of the preferred embodiment according to the present invention records the disk identification information carrying out the recording operation and the reproducing operation into the user data area for each optical disk in a read-only area which is not rewritable, and therefore, the optical disk thereof can control the recording operation and the reproducing operation of the contents onto the optical disk by the user by using the information recorded upon manufacturing the optical disk.

**[0070]** An optical disk of the preferred embodiment according to the present invention can prevent the disk identification information from being copied in order to make the correct decoding and reproduction of the data impossible even in the case where the user data area information is copied by the user onto a different recording-type of optical disk by recording the encrypted data in the user data area of the optical disk with a key of the disk identification information of read-only which is impossible to be rewritten.

**[0071]** An optical disk of the preferred embodiment according to the present invention makes it possible to carry out independently (a) acquisition of the data which need copyright protection such as movies, music and (b) acquisition of the descramble key for decrypting the encryption, by recording the encrypted data and the descramble key for decrypting the encryption in different sector areas. In addition, by encrypting and recording the descramble key with a key of the disk identification information, even in the case where the user data area information is copied onto another recording-type optical disk by the user, the disk identification information cannot be copied, and correct decoding and reproduction of the data becomes impossible and by acquiring and recording the encrypted descramble key with a key of the disk identification information on the optical disk where it is copied, correct decoding and reproduction of the data can be made possible.

## THIRD PREFERRED EMBODIMENT

**[0072]** Next, an encrypted content recording and reproducing method of a third preferred embodiment according to the present invention will be described in reference to the drawings. Fig. 16 shows a plan view illustrating a data recording area of an optical disk 1101 of the third preferred embodiment according to the present invention.

**[0073]** Referring to Fig. 16, 1101 denotes a recording medium which can record digital data, and which is a recording-type optical disk such as a rewritable or non-rewritable optical disk, 1102 denotes a control user data area in which disk information is recorded in a form of minute concavo-convex pits, and 1103 denotes a user data area in which the user records data by irradiating a light beam of laser onto the optical disk. 1104 denotes an BCA in which disk ID is recorded. In the BCA 1104, a recording film on minute concavo-convex pits in an inner periphery section of the control user data area 1102 is trimmed by partially irradiating a laser beam of pulse laser such as a YAG laser or the like onto the recording film, so that a plurality of trimming areas 1105 is formed in an elongated shape in the radius direction, thereby to record a disk ID which is the descrambled identification information.

**[0074]** Fig. 17 is a waveform diagram showing a signal waveform of a reproduced signal 1201 and a reproduced binarized signal 1207 in a BCA reproducing circuit 1401 according to the third preferred embodiment, and Fig. 18 shows a block diagram illustrating a configuration of the BCA reproducing circuit 1401 according to the thirdpreferred embodiment. Fig. 17 shows a re-

producing signal 1201 when data of the BCA 1104 is reproduced. In Fig. 18, 1301 denotes an optical pickup, 1302 denotes a pre-amplifier, 1303 denotes a low-pass filter (LPF), 1304 denotes a binarizing circuit, and 1305 denotes a demodulation circuit.

**[0075]** Referring to Fig. 18, a laser beam outputted from the optical pickup 1301 irradiates the BCA 1104 of the optical disk 1101, and the reflected light is photoelectrically converted by the optical pickup 1301, and thereafter, an electric signal which has been photoelectrically converted is amplified by the pre-amplifier 1302 to obtain a reproduced signal 1201. In this case, the reproduced signal 1201 shown in Fig. 17 has a level corresponding to the concavo-convex pits of the control user data area 1102, and in this reproduced signal 1201, each of 1202, 1203 and 1204 denotes a trimming portion where signals in a form of concavo-convex pits drop out when the recording film is removed by the trimming process by the pulse laser. This trimming process is carried out by the manufacturer of the optical disk.

**[0076]** Referring back to Fig. 18 for the description, the reproduced signal 1201 is inputted to the low-pass filter 1303, which then removes the modulated signal formed by the concavo-convex pits, and thereafter, outputs a resulting signal to the binarizing circuit 1304. The reproduced signal inputted into the binarizing circuit 1304 is binarized by using a slice level 1206 which is a level significantly lower than the slice level 1205 instead of the normal slice level 1205 which binarizes a signal of control user data area 1102, to obtain the reproduced binarized signal 1207. The reproduced binarized signal 1207 outputted from the binarizing circuit 1304 is demodulated by a demodulation circuit 1305, to obtain the disk ID signal 1306.

**[0077]** As described above, by adding the disk identification information for identifying an optical disk, management of the optical disk can be easily implemented. Also, by recording the BCA 1104 in a form of concavo-convex pits, the information for identifying the optical disks within the BCA 1104 can be prevented from being easily falsified. In addition, since the control user data area 1102 and the BCA 1104 shown in Fig. 16 are adjacent from each other, the data of the BCA 1104 can be continuously reproduced when the data of the control user data area 1102 are reproduced, or the data of the control user data area 1102 can be continuously reproduced when the data of the BCA 1104 are reproduced, and therefore, it becomes possible to accelerate the process for obtaining the information of the BCA 1104 for identifying optical disks quickly by the CPU when, for example, the optical disk is started up, and for recording the encrypted content.

**[0078]** Although the BCA 1104 of the preferred embodiment is formed so as to trim the recording film in a form of concavo-convex pits in the inner periphery section of the control user data area 1102, the recording film, which constitutes an optical disk of recording type which is either a rewritable or non-rewritable optical disk, is easily affected by heat as compared with the reflecting film formed on a read-only optical disk. By trimming the inner periphery section of the control user data area 1102, the user data area 1103 can be protected from the heat emitted upon trimming as compared with the case where the outer periphery section is trimmed. Also, the reason why the BCA 1104 is formed on the inner peripheral side of the control user data area 1102 is that a margin should be taken into consideration in the case that the diameter of the spot of a laser beam changes due to the instability of a focusing servo circuit of the laser device.

**[0079]** The data recorded in the BCA 1104 before trimming may be recorded in the control user data area 1102. The data recorded in the BCA 1104 are also recorded in the control user data area 1102, and this leads to that the above data of the control user data area 1102 can be protected from the trimming. In addition, when the data recorded in the BCA 1104 is recorded continuously and repetitively from the BCA 1104 to the control user data area 1102, the position of the BCA 1104 can be predicted by finding the above data of the control user data area 1102.

**[0080]** Next, the procedure for recording the encrypted content by the disk ID through a network on an optical disk 1101 having the above-mentioned BCA 1104 will be described. In the third to fifth preferred embodiments, a network means, for example, the Internet, the public telephone line or the other communication lines such as leased lines or circuits. Fig. 19 shows a block diagram illustrating a configuration of an optical disk recording and reproducing system according to the third preferred embodiment, and illustrates an apparatus configuration for recording encrypted contents on an optical disk of recording type 1101, which is either a rewritable or non-rewritable optical disk having the above-mentioned BCA 1104.

**[0081]** Referring to Fig. 19, an optical disk recording and reproducing system is constituted by comprising an optical disk recording and reproducing apparatus 1410, and an encryption section 1406 connected to each other through a network 1405 such as the Internet. The optical disk recording and reproducing apparatus 1410 comprises an optical pickup 1301, a BCA reproducing circuit 1401, the Internet 403, a recording circuit 1411, a data reproducing section 1412 and an encryption decoder 1413. Also, the encryption section 1406 comprises an interface 1404, a content memory 1407, and an encryption encoder 1408.

**[0082]** First of all, a laser beam outputted from the optical pickup 1301 irradiates, for example, the BCA 1104 of the RAM type optical disk 1101, and then, after the reflected light is photoelectrically converted by the optical pickup 1301, a reproduced signal which has been photoelectrically converted is inputted to the BCA reproducing circuit 1401. The BCA reproducing circuit 1401 reproduces a disk ID signal 1402 within the BCA based on the inputted reproduced signal, outputs the repro-

duced disk ID signal 1402 to the encryption decoder 1413, and also simultaneously output the same disk ID signal 1402 to the encryption encoder 1408 of the encryption section 1406 via the interface 1403 and 1404 as well as the network 1405. The encryption encoder 1408 encrypts data of content or scrambles data of content for image and speech sound, so that the disk ID signal 1402 becomes a decipher key for decrypting the encryption on the optical disk 1101 where the data of the content within the content memory 1407 is recorded.

**[0083]** In the present preferred embodiment, a process of encrypting the content 1407 using the disk ID signal 1402 as a cipher key means the same as the encrypting process. Also, in the present preferred embodiment, encrypting and decrypting are considered as a relationship between a lock and a key, so that closing the lock with the key is referred to encrypting and opening the lock with the key is referred to decrypting. Accordingly, encrypting and decrypting differ in the actual operation from each other, however, the keys for encrypting and for decrypting are the same as each other. The content 1407 is denoted by C, the disk ID signal 1402 is denoted by BCAS, the encrypted content 1409 is denoted by C[BCAS], and the operation for the encrypting process is denoted by * . Then the following equation can be represented:

$$C * BCAS = C\,[BCAS] \qquad (1).$$

**[0084]** The content 1409 encrypted by the encryption section 1406 is sent to a recording circuit 1411 of the recording and reproducing apparatus 1410 via the interface 1403 and 1404 as well as the network 1405. The recording circuit 1411 digitally modulates data of the inputted content in a predetermined manner, and records the data of the content onto the optical disk 1101 by modulating the intensity of the laser beam from the optical pickup 1301 corresponding to the digitally modulated data and irradiating the laser beam onto the optical disk 1101.

**[0085]** Next, when the above content encrypted and recorded on the optical disk 1101 is reproduced, a laser beam outputted from the optical pickup 1301 irradiates the area where the above encrypted content of the user data area 1103 is recorded, and after the reflected light is photoelectrically converted by the optical pickup 1301, the reproduced signal which has been photoelectrically converted is inputted to the data reproducing section 1412. The data reproducing section 1412 A/D converts the inputted reproduced signal into digital data, and outputs the digital data to the encryption decoder 1413. On the other hand, a laser beam from the optical pickup 1301 is irradiated onto the BCA 1104 of the optical disk 1101, and after the reflected light is photoelectrically converted by the optical pickup 1301, the reproduced signal which has been photoelectrically converted is inputted to the BCA reproducing circuit 1401. The BCA reproducing circuit 1401 A/D converts the inputted reproducing signal to generate the disk ID signal 1402, and then, the disk ID signal 1402 is outputted to the encryption decoder 1413.

**[0086]** The encryption decoder 1413 uses the inputted disk ID signal 1402 as a key for decrypting the data of the encrypted content. At this time, when the content is regularly recorded on the optical disk 1101, the key for decrypting the encrypted content recorded on the optical disk 1101 is the disk ID signal 1402 of the optical disk 1101, and the disk ID signal 1402 outputted from the BCA reproducing circuit 1401 upon reproduction is also the disk ID signal (BCAS) of the optical disk 1101. Accordingly, the content which is either decrypted or descrambled is outputted from the encryption decoder 1413 as an output signal 1414. When the operation for the decoding process is denoted by #, the following equation can be represented:

$$C\,[BCAS] \,\#\, BCAS = C \qquad (2).$$

**[0087]** In this case, when data of the content is image data, the image data such as an MPEG signal is expanded to obtain data of an image signal.

**[0088]** As described above, the encrypting of the present preferred embodiment has a disk ID as a key, and since only one disk ID exists corresponding to one optical disk, there is such an advantageous effect that the same encrypted content can be recorded only on that optical disk. That is to say, when the above describe that content 1407 is attempted to be copied and reproduced onto another optical disk which has another disk ID of ID2 from a regular optical disk which has, for example, a disk ID of ID1, ID2 is outputted as the disk ID signal 1402 from the BCA reproducing circuit 401. However, the encrypted content is encrypted with a disk ID signal of ID1, therefore, the encrypted content can not be decoded by the encryption decoder 1413.

**[0089]** The encrypting encoder 1408 is not located at a supplying source of the content, and is located on the side of the recording and reproducing apparatus in the network, then it may be formed in a form of an IC card or the like on which the encrypting encoder is mounted. Also, since the above-mentioned optical disk 1101 is encrypted using only the disk ID, data can be reproduced with an arbitrary optical disk recording and reproducing apparatus having the BCA reproducing circuit 1401 and the encryption decoder 1413.

## FOURTH PREFERRED EMBODIMENT

**[0090]** Next, an encrypted content recording method of the fourth preferred embodiment according to the present invention will be described in reference to the drawings. Fig. 20 is a block diagram illustrating a configuration of an optical disk recording and reproducing system of a fourth preferred embodiment according to

the present invention, which shows an apparatus configuration for recording encrypted content on a recording-type optical disk which is either rewritable or non-rewritable optical disk having a BCA. In the description of the fourth preferred embodiment, the description for the elements shared with the third preferred embodiment are omitted.

**[0091]** Referring to Fig. 20, the optical disk recording and reproducing system according to the fourth preferred embodiment comprises a CATV company apparatus 1501, a key issuing center apparatus 1507, a CATV decoder 1506, an optical disk recording and reproducing apparatus 1514, and a television set 1530. In this case, the CATV company apparatus 1501 comprises a content memory 1502 for storing data of content such as movie software, a first cipher key memory 1503 for storing a first cipher key and a first cipher encoder 1504. Also, the key issuing center apparatus 1507 comprises a control section 1507a for controlling the operation of the apparatus 1507, a time limiting information memory 1510 for storing time limiting information, and a recording admission code memory 1511 for storing a limiting admission code. In addition, the CATV decoder 1506 comprises a system ID memory 1508 for storing a system ID of the CATV decoder 1506, a first cipher decoder 1513, a second cipher encoder 1516, and a company identification signal memory 1523 provided within an IC card 1522. Furthermore, the optical disk recording and reproducing apparatus 1514 comprises a recording circuit 1518, a data reproducing section 1519, a BCA reproducing circuit 1521, a second cipher decoder 1520, and a company identification signal memory 1526 provided within an IC card 1524.

**[0092]** First of all, the first cipher encoder 1504 of the CATV company apparatus 1501 encrypts the data of the content stored in the content memory 1502, such as movie software, using a first cipher key stored in the first cipher key 1503, thereby to generate a first encrypted content 1505. Then the generated first encrypted content 1505 is transmitted to the first cipher decoder 1513 of the CATV decoder 1506 for each user via the network. When the data stored in the content memory 1502 is denoted by C, the first cipher key 1503 is denoted by FK, and the first encrypted content 1505 is denoted by C[FK], then the following equation can be represented:

$$C * FK = C[FK] \quad (3).$$

**[0093]** The CATV decoder 1506 transmits, via the network to the key issuing center apparatus 1507,

(a) a system ID for the CATV decoder 1506 stored in the system ID memory 1508; and
(b) a title code 1509 inputted by using, for example, a keyboard (not shown) of the CATV decoder 1506, which is added in advance to the above-mentioned content desired to be recorded on the audio-type or RAM-type optical disk 1101. In this case, the title code 1509 may be inputted by being selected according to the TV screen or may be inputted directly using the keyboard or may be inputted from a remote controller or the like. Accordingly, the title code 1509 may be obtained by user's acquisition in his own way, or may be to the CATV decoder 1506 together with the first encrypted content 1505. The title code 1509 may be sent in advance at a different time from that of the first encrypted content 1505 in a form such as a program guide.

**[0094]** Based on the system ID of the CATV decoder 1506 and the title code 1509 of the above-mentioned content, the control section 1507a of the key issuing center apparatus 1507 refers to the time limiting information stored in the time limiting information memory 1510 and the recording admission code stored in the recording admission code memory 1511, and transmits a key (K) 1512 corresponding to these data of the recording admission code and the time limiting code, together with the recording admission code and the time limiting code, via the network to the first cipher decoder 1513 of the CATV decoder 1506. The time limiting information allows the same content to be distinguished among the cases where the same content is broadcasted a plurality of times at different times. When the first decipher key is denoted by FK, the system ID of the CATV decoder 1506 is denoted by DID, the time limitation information is denoted by TIME, the recording admission code is denoted by COPY, and the title code 1509 of the content is denoted by T. Then, the key (K) satisfies the relationship indicated by the following equation:

$$FK = K * T * DID * TIME * COPY \quad (4).$$

**[0095]** It is determined whether the recording admission code stored in the record permission code memory 1511 is permitted only for watching and listening, or for both of watching and listening, and recording, based on a judgment result when the CATV company apparatus 1501, for example, judges whether or not the broadcast content is a new work or an old work.

**[0096]** The first cipher decoder 1513 of the CATV decoder 1506 decrypts the first encrypted content 1505 when the first decipher key (FK), the key (K) 1512, the title code 1509 of the above-mentioned content, the system ID, the record permission code and the time limitation information satisfy the above-mentioned relationship, and the present time information outputted from the clock circuit 1527 satisfies the condition of the time limitation information. In this case, when the above-mentioned encrypted content are an image signal, the descrambled image signal is outputted from the first cipher decoder 1513 to the television set 1530, and then the user can watch an image of the image signal and

listen to an audio signal corresponding to the image signal. In this case, the decrypting process of the first cipher decoder 1513 is expressed by the following equation:

$$C\ [FK]\ \#\ (K*T*DID*TIME*COPY)$$

$$= C\ [FK]\ \#\ FK$$

$$= C \qquad (5).$$

**[0097]** When the record permission code permits only watching and listening, the content data can be recorded on the optical disk 1101, however, when both of watching and listening, and recording are permitted, the content data can be recorded on the optical disk 1101. Therefore, this method will be described as follows.

**[0098]** The BCA reproducing circuit 1521 of the optical disk recording and reproducing apparatus 1514 reproduces the data of the BCA 1104 of the optical disk 1101 to obtain the disk ID signal 1515, and outputs the disk ID signal to the second cipher encoder 1516 of the CATV decoder 1506. The second cipher encoder 1516 of the CATV decoder 1506 encrypts the data of the content outputted from the first cipher decoder 1513, using the disk ID signal 1515 as the second cipher key to generate a second encrypted content 1517, and outputs the generated second encrypted content 1517 to the recording circuit 1518 of the optical disk recording and reproducing apparatus 1514. It is to be noted that the above-mentioned encrypting of the second cipher decoder 1516 is limited to the time when the first encrypted content is decrypted and outputted from the first cipher decoder 1513. The content which is the output signal from the first cipher decoder 1513 is denoted by C, the disk ID signal 1515 which is the second cipher key is denoted by BCAS, and the second encrypted content 1517 is denoted by C[BCAS], then the following equation can be represented:

$$C * BCAS = C\ [BCAS] \qquad (6).$$

**[0099]** The second encrypted content 1517 sent to the recording circuit 1518 of the optical disk recording and reproducing apparatus 1514 is modulated using, for example, a well known 8/16 modulation system to the recording circuit 1518, and then, the modulated signal is recorded in the user data area 1103 on the optical disk 1101 by the optical pickup (not shown). When the above-mentioned content encrypted and recorded on the optical disk 1101 is reproduced, the laser beam outputted from the optical pickup is irradiated onto an area where the above-mentioned encrypted content is recorded on the optical disk 1101, so that the reflected light enters the optical pickup. The above-mentioned optical pickup photoelectrically converts the entered reflected light into a reproduced electric signal, and then, the reproduced signal which has been photoelectrically converted is outputted to the data reproducing section 1519. The data reproducing section 1519 A/D converts the inputted reproduced signal into a digital reproduced signal, and then, the digital reproduced signal is outputted the second cipher decoder 1520.

**[0100]** On the other hand, a laser beam outputted from the optical pickup is irradiated onto the BCA 1104 of the optical disk 1101, so that the reflected light enters the optical pickup. The above-mentioned optical pickup photoelectrically converts the inputted reflected light into a reproduced electric signal, and then, the reproduced signal which has been photoelectrically converted is outputted to the BCA reproducing circuit 1521. The BCA reproducing circuit 1521 generates the disk ID signal 1515 based on the inputted reproduced signal, and the generated disk ID signal is outputted to the second cipher decoder 1520. In response to the disk ID signal, the second cipher decoder 1520 decrypts the reproduced encrypted content from the data reproducing section 1519, using the inputted disk ID signal 1515 as a key. At that time, in the case that the content is regularly recorded on the optical disk 1101, the key for decrypting the encrypted content recorded on the optical disk 1101 is the disk ID of the optical disk 1101, and the disk ID signal outputted from the BCA reproducing circuit 1521 is also the disk ID signal (BCAS) of the optical disk 1101, and therefore, the second cipher decoder 1520 can normally carry out the decrypting process. Accordingly, the data of the content decrypted or descrambled are outputted from the second cipher decoder 1520 as an output signal 1525. In this case, the decrypting process of the second cipher decoder 1520 can be expressed in the following equation. When the data content is an image signal, the second cipher decoder 1520 expands, for example, an MPEG signal to reproduce an original image signal, and then, outputs the image signal.

$$C\ [BCAS]\ \#\ BCAS = C \qquad (7)$$

**[0101]** The above-mentioned optical disk 1101 is encrypted using only the disk ID signal (BCAS) 1515, and therefore, it is possible to reproduce content data by an arbitrary optical disk recording and reproducing apparatus comprising a BCA reproducing circuit 1521 and the second cipher decoder 1520. Although the encryption encoders 1504 and 1516 perform encryption and the encryption decoders 1513 and 1520 perform decryption in the above description, encrypting and decrypting may be performed by such a configuration that programs for encryption algorithms and decryption algorithms are included in the program carried out by the CPU which is the control section within each of the apparatuses 1501, 1506 and 1514.

**[0102]** Although, in the present preferred embodiment, the second cipher encoder 1516 of the CATV decoder 1506 encrypts the content using the disk ID signal

1515 as the second cipher key, the content may be encrypted as follows. For example, the IC card 1522 prepared for each CATV company apparatus 1501 may be mounted on the CATV decoder 1506, and the company identification signal recorded within the company identification signal memory 1523 of the IC card 1522 and the disk ID signal (BCAS) reproduced by the BCA reproducing circuit 1521 may be combined to be used as the second cipher key for encrypting the content by the second cipher encoder 1516. The content of the output signal from the first cipher decoder 1513 is denoted by C, the disk ID signal 1515 which is the first second cipher key is denoted by BCAS, the company identification signal 1523 which is the second cipher key is denoted by CK, and the second encrypted content 1517 is denoted by C[BCAS, CK]. Then, the encrypting process of the second cipher encoder 1516 is expressed by the following equation:

$$C * BCAS * CK = C\,[BCAS, CK] \qquad (8).$$

**[0103]** Next, when the content encrypted and recorded on the optical disk 1101 is reproduced, a laser beam outputted from the optical pickup is irradiated onto an area in which the above encrypted content has been recorded on the optical disk 1101, so that the reflected light enters the optical pickup. The optical pickup photoelectrically converts the entered reflected light to a reproduced signal, which is then outputted to the data reproducing section 1519. The data reproducing section 1519 A/D coverts the inputted reproduced signal into a digital reproduced signal, which is then outputted to the second cipher decoder 1520. On the other hand, a laser beam outputted from the optical pickup is irradiated onto the BCA 1104 of the optical disk 1101 so that the reflected light enters the optical pickup. The optical pickup photoelectrically converts the entered reflected light into a reproduced signal, which is outputted to the BCA reproducing circuit 1521. The BCA reproducing circuit 1521 reproduces the disk ID signal 1515 based on the inputted reproduced signal, and then, the disk ID signal 1515 is outputted to the second cipher encoder 1516 and the second cipher decoder 1520.

**[0104]** In addition, the company identification signal stored in the company identification signal memory 1526 of the IC card 1524 mounted on the optical disk recording and reproducing apparatus 1514 is inputted to the second cipher decoder 1520. The company identification signal may not be recorded within the company identification signal memory 1526 of the IC card 1524, for example, upon installation of a recording program of the optical disk recording and reproducing apparatus 1514, the company identification signal may be recorded in a memory (not shown) connected to a CPU of a control section of the optical disk recording and reproducing apparatus 1514. Alternatively, the company identification signal may be inputted using a keyboard (not shown) of the optical disk recording and reproducing apparatus 1514.

**[0105]** The second cipher decoder 1520 decrypts the encrypted content using the inputted disk ID signal 1515 and the company identification signal as decipher keys. At this time, in the case that the user of the CATV decoder 1506 contracts formally with a particular CATV company having the CATV company apparatus 1502, and the content 1502 is regularly recorded on the optical disk 1101, the first decipher key for the encrypted content encrypted and recorded on the optical disk 1101 is just the disk ID signal (BCAS) of the optical disk 1101 which will be reproduced exactly at that moment, and the second cipher key is the company identification signal (CK) stored in the company identification signal memory 1526 of the IC card 1524 supplied from the contracted CATV company. Accordingly the outputted signal 1525 of the decoded or descrambled contents is outputted from the second cipher decoder 1520. In this case, the decrypting process of the second cipher decoder 1520 is expressed in the following equation. When the content is an image signal, for example, an MPEG signal is extended by the second cipher decoder 1520, and then, an output signal 1525 of the image signal is outputted.

$$C\,[BCAS, CK]\ \#\ (BCAS * CK) = C \qquad (9)$$

**[0106]** Since the content of the above optical disk 1101 is encrypted using the disk ID signal 1515 and the company identification signal, it is possible to carry out reproduction by an arbitrary optical disk recording and reproducing apparatus comprising the BCA reproducing circuit 1521 and the second cipher decoder 1520 if the contract is made with the CATV company which supplies the above-mentioned content. On the contrary, if the contract is not made with above-mentioned CATV company, the company identification signal cannot be obtained, and the content cannot be reproduced, then this makes it possible to distinguish the contracted user from non-contracted user.

**[0107]** Also, since in the present preferred embodiment each user sends a disk ID signal from the optical disk recording and reproducing apparatus 1514 to the CATV decoder 1506 located at their own home to encrypt image data or the like, it is not necessary for the CATV apparatus 1501 to change encrypted content individually delivered to each user, therefore, the system for broadcasting can be simplified to supply the same content to a mass audience at low cost. In addition, according to the present preferred embodiment, recording on only one RAM-type optical disk can be permitted for each user having the CATV decoder 1506.

**[0108]** Although, in the present preferred embodiment, the case where the content is broadcasted from a head end of the cable television system is described, the present invention is not limited to this, the present

invention can be applied to broadcasting using radio wave.

FIFTH PREFERRED EMBODIMENT

**[0109]** A method for recording and reproducing encrypted content of a fifth preferred embodiment according to the present invention will be described in reference to the drawings. Fig. 21 shows a plan view illustrating a data recording area of an optical disk 1601 of the fifth preferred embodiment according to the present invention, and Fig. 22 is a block diagram showing a configuration of an optical disk recording and reproducing system according to the fifth preferred embodiment. In the fifth preferred embodiment, the description for the common elements with the third and the fourth preferred embodiments are omitted in the following description.

**[0110]** Referring to Fig. 21, 1601 denotes a recording-type optical disk which is either a rewritable type or non-rewritable type of optical disk, 1602 denotes a control user data area in which disk information is recorded in a form of concavo-convex pits, 1603 denotes a user data area into which the user record the data by irradiating a light beam from a laser onto the optical disk, and 1604 denotes an BCA in which a disk ID is recorded.

**[0111]** In the BCA 1604, a plurality of trimming areas 1606 having an elongated shape in the radius direction are formed by partially trimming a recording film on concavo-convex pits in the inner peripheral section of the control user data area 1602 using a pulse laser such a YAG laser or the like. The trimming is carried out by the disk manufacturer. Also, by adding the disk ID to the data recorded in the BCA 1604, the management of the optical disk can be easily implemented. In addition, by recording the data of the BCA 1604 on the concavo-convex pits, the information for identifying the optical disk which is recorded in the BCA 1604 can be prevented from easily being falsified.

**[0112]** In addition, by arranging the control user data area 1602 and the BCA 1604 so as to be adjacent from each other, the data of the BCA 1604 can be reproduced continuously when the data of the control user data area are reproduced or the data of the control user data area can be reproduced continuously when the data of the BCA 1604 are reproduced, therefore, it becomes possible to accelerate the process for obtaining or acquiring information of the BCA 1604 so as to identify the optical disk quickly by the CPU, for example, when the optical disk is started up and for recording the encrypted contents.

**[0113]** Although the BCA 1604 of the present preferred embodiment is formed by trimming the recording film on the concavo-convex pits in the inner periphery section of the control user data area 1602, the recording film which constitutes an optical disk of recording type which is either a rewritable type or non-rewritable-type of optical disk is easily affected by heat, as compared with the reflecting film formed on a read-only optical disk. By trimming the inner periphery section of the control user data area 1602, the recording data of the user data area 1603 can be protected from the heat generated upon trimming as compared with that when the outer periphery section is trimmed. The reason why the BCA 1604 is formed on the inner peripheral side of the control user data area 1602 is that a margin is taken into consideration, when the diameter of the beam spot from a laser beam fluctuates due to instability of a focusing servo circuit of a laser device. The data recorded in the BCA 1604 before trimming may be recorded in the control user data area 1602. The data recorded in the BCA 1604 can be recorded in the control user data area 1602 so that the above-mentioned data of the control user data area 1602 can be protected upon trimming.

**[0114]** In addition, when the above-mentioned data is recorded continuously and repetitively from the BCA 1604 to the control user data area 1602, the position of the BCA 1604 can be predicted by finding out the above-mentioned data in the control user data area 1602. Also, the data in the key information recording area 1605 is recorded by irradiating a light beam in the same way as that of the user data area 1603.

**[0115]** In a manner similar to that of the present preferred embodiment, by arranging the control user data area 1602 and the key information recording area 1605 so as to be adjacent from each other, the data in the key information recording area 1605 can be reproduced continuously when the data of the control user data area 1602 are reproduced or the data of the control user data area 1602 can be reproduced continuously when the data of the key information recording area 1605 are reproduced, therefore, it becomes possible to accelerate the process for obtaining the information of the BCA 1604 to identify the optical disk quickly by a CPU when, for example, the optical disk is started up and for reproducing the encrypted content.

**[0116]** Referring to Fig. 22, the optical disk recording and reproducing system according to the fifth preferred embodiment comprises a CATV company apparatus 1701, a key issuing center apparatus 1707, a CATV decoder 1706, an optical disk recording and reproducing apparatus 1714, and a television set 1730. In this case, the CATV company apparatus 1701 comprises a content memory 1702 for storing the content such as movie software, a first cipher key memory 1703 for storing a first cipher key and a first cipher encoder 1704. Also, the CATV decoder 1706 comprises a system ID memory 1708, a first cipher decoder 1713, and a clock circuit 1725 for outputting the present time information. Further, the key issuing center apparatus 1707 comprises a control section 1707a for controlling the operation of the apparatus 1707 and a time limiting information memory 1710. Further, the optical disk recording and reproducing apparatus 1714 comprises a recording circuit 1717, a key information recording circuit 1719, a BCA reproducing circuit 1720, a data reproducing section 1721, a second cipher decoder 1722 and a key informa-

tion reproducing section 1723.

**[0117]** First of all, the first cipher encoder 1704 of the CATV apparatus 1701 encrypts data of content such as movie software which is stored in the content memory 1702, using the first cipher key 1703, so as to generate a first encrypted content 1705, and transmits the generated first encrypted content 1705 to the first cipher decoder 1713 of the CATV decoder 1706 of each user through the network. The content stored in the content memory 1702 is denoted by C, the first cipher key stored in the first cipher key memory 1703 is denoted by FK, and the first encrypted content 1705 is denoted by C [FK], then, the following equation can be represented:

$$C * FK = C [FK] \quad (10).$$

**[0118]** The CATV decoder 1706 transmits to the control section 1707a of the key issuing center apparatus 1707 via the network, a system ID stored in the system ID memory 1708 of the CATV decoder 1706, and a title code 1709 of the above-mentioned content which user wishes to watch and listen to where the title code 1709 is inputted by using, for example, a keyboard (not shown). The above-mentioned title code may be inputted by selecting according to the screen of the television set 1730, may be inputted directly using the keyboard or may be inputted from the remote controller or the like. Accordingly, the title code may be obtained by a user in his way, may be sent from the CATV decoder 1706 together with the first encrypted content or may be sent in advance at different time from that of the first encrypted content in a form of program guidance or the like.

**[0119]** Based on the system ID of the CATV decoder 1706 and the title code of the above-mentioned content, the control section 1707a of the key issuing center apparatus 1707 generates the corresponding key (K) 1712 in reference to the corresponding time limitation information stored in the time limitation information memory 1710, and then, transmits the generated key (K) 1712 to the first cipher decoder 1713 of the CATV decoder 1706 via a network. The time limitation information makes it possible to distinguish among the cases where the same content is broadcasted a plurality of times at different times. The first decipher key is denoted by FK, the system ID of the CATV decoder 1706 is denoted DID, the time limitation information is denoted by TIME, and the title code of the content is denoted by T, the key (K) 1712 satisfies the relationship represented by the following equation:

$$FK = K * T * DID * TIME \quad (11).$$

**[0120]** The first cipher decoder 1713 can decrypt the first encrypted content 1705 if the first decipher key (FK), the above key (K) 1712 transmitted from the key issuing center apparatus 1701, the title code of the above-mentioned content, the system ID, and the time limitation information satisfy the above-mentioned relationship and the time limitation information satisfies the condition of the present time information from the clock circuit 1725. In this case, when the first encrypted content 1705 is an image signal, the descrambled image signal is outputted to the television set 1730 from the first decipher decoder 1713, so that the user can watch and listen to the content on the television set 1730. In this case, the decrypting process of the first cipher decoder 1713 is expressed as follows:

$$C [FK] \# (K * T * DID * TIME)$$

$$= C [FK] \# FK$$

$$= C \quad (12)$$

**[0121]** Next, the method for recording the above-mentioned content on the optical disk 1601 will be described. When the content is recorded on the optical disk 1601, the first encrypted content 1705 which has not been decrypted by the CATV decoder 1706 is transmitted to the recording circuit 1717 of the optical disk recording and reproducing apparatus 1714 from the first cipher encoder 1704 of the CATV company apparatus 1701. The recording circuit 1717 digitally modulates data of the received first encrypted content 1705 by using a modulation system such as a well known 8/16 modulation system, and the modulated digital data are recorded on the optical disk 1601 by the optical pickup (not shown). Accordingly, it is necessary for the first encrypted content 1705 to be decrypted in order to reproduce the above-mentioned content encrypted and recorded on the optical disk 1601.

**[0122]** The optical disk recording and the reproducing apparatus 1714 transmits to the control section 1707a of the key issuing center apparatus 1707 via the network, the disk ID signal 1715 of the optical disk 1601 reproduced by the BCA reproducing circuit 1720 and the title code 1716 of the above-mentioned content, which is inputted using, for example, a keyboard (not shown) and which the user wishes to reproduce. As to the timing for sending the disk ID, the disk ID may be sent when the key issuing center apparatus 1707 is accessed or the disk ID may be sent together with the title code when listening and watching the content.

**[0123]** Although as a method for transmitting the disk ID, a method for sending the output signal from the BCA reproducing circuit 1720 directly to the key issuing center apparatus 1707 by reproducing the BCA 1604 of the optical disk 1601 as shown in Fig. 22 is disclosed above, the present invention is not limited to this, the following method may be used. For example, the data of the BCA 1604 is reproduced before access to the key issuing center apparatus 1707 when starting up the disk, and the data of the BCA 1604 is stored in a memory (not

shown) of the optical disk recording and reproducing apparatus 1714 or the CATV decoder 1706, then, it is transmitted to the control section 1707a of the key issuing center apparatus 1707 at the above-mentioned timing. In addition, when the disk ID can be recognized visually in some form such as a label, a keyboard may be used for inputting the disk ID. When the label is a bar code, a bar code reader may be used for reading out the disk ID.

**[0124]** The control section 1707a of the key issuing center apparatus 1707 generates a key (DK) 1718 corresponding to the disk ID signal 1715 of the optical disk 1601 and the title code 1716 of the content, and transmits the generated key (DK) 1718 to the key information recording circuit 1719 of the optical disk recording and reproducing apparatus 1714. In this case, the first decipher key is denoted by FK, the disk ID signal 1715 of the optical disk 1601 is denoted by BCAS, and the title code 1716 of the content is denoted by T, the key (DK) satisfies the relationship of the following equation:

$$FK = DK * BCA * T \quad (13).$$

**[0125]** The key (DK) inputted into the key information recording circuit 1719 of the optical disk recording and reproducing apparatus 1714 is digitally modulated using a modulating system such as the well known 8/16 modulation system or the like, and then, the modulated digital data is recorded in the key information recording area 1605 on the optical disk 1601 by the optical pickup (not shown). The key (DK) may be recorded a plurality of times in the key information recording area 1605. By recording the same key a plurality of times, the key (DK) can be protected when the recording film of the key information recording area 1605 deteriorates or when the optical disk 1601 gets scratched, so that the content can be decrypted only when the data of either one of the keys (DK) can be reproduced.

**[0126]** Although in the present preferred embodiment, the key information recording area 1605 is provided on the inner peripheral side of the user data area 1603, it may be provided on the outer peripheral side of the user data area 1603 or may be provided both on the inner periphery and the outer peripheral sides. By providing the key information recording area 1605 n the outer peripheral side, it becomes possible to record more keys (DK). Also, by dispersedly providing a plurality of key information recording areas, the key (DK) can be protected by the other key information recording areas even in the case that one key information recording area cannot be reproduced.

**[0127]** On the other hand, a laser beam outputted from the optical pickup is irradiated onto the area of the optical disk 1601 on which the above content is recorded so that the reflected light enters into the optical pickup. The optical pickup photoelectrically converts the entered reflected light into a reproduced electric signal, and the reproduced signal which has been photoelectrically converted is outputted to the data reproducing section 1721. In response to this, the data reproducing section 1721 A/D converts the inputted reproduced signal into encrypted digital data, which is outputted to the second cipher decoder 1722. In addition, a laser beam outputted from the optical pickup is irradiated onto the BCA 604 of the optical disk 1601, and then, the reflected light enters the optical pickup. The optical pickup photoelectrically converts the inputted reflected light into a reproduced electric signal, and the reproduced signal which has been photoelectrically converted is outputted to the BCA reproducing circuit 1720. In response to this, the BCA reproducing circuit 1720 reproduces the disk ID signal 1715 based on the inputted reproduced signal, which is outputted to the encryption decoder 1722. In addition, a laser beam outputted from the optical pickup is irradiated onto the key information recording area 1605 of the optical disk 1601 so that the reflected light enters the optical pickup. The optical pickup photoelectrically converts the entered reflected light into a reproduced electric signal, and outputs the reproduced signal to the key information reproducing section 1723. In response to this, the key information reproducing section 1723 generates data of a key (DK) based on the inputted reproduced signal, which is outputted to the second cipher decoder 1722.

**[0128]** When the content is reproduced immediately after access to the key issuing center apparatus 1707, the key information recording circuit 1719 may directly input the key (DK) to the second cipher decoder 1722 before recording the same key (DK) in the key information recording area 1605. By doing this, the time until the reproduction is started can be shortened. The cipher decoder 1722 decrypts the encrypted content using the decipher key including the inputted disk ID signal 1715, the key (DK) and the title code 1716 of the above content. The decrypting process of the second cipher decoder 1722 is expressed in the following equation. When the content is an image signal, an MPEG signal is, for example, expanded so that an output signal 1724 of the image signal is outputted from the second cipher decoder 1722.

$$\begin{aligned} C\,[FK]\,\#\,(DK * BCA * T) \\ = C\,[FK]\,\#\,FK \\ = C \end{aligned} \quad (14)$$

**[0129]** In the present preferred embodiment, when a user fee is imposed when the key signal is received from the control section 1707a of the key issuing center apparatus 1707, a fee is separately imposed when listening and watching the content, and the content recorded on the optical disk 1601 is reproduced for the first time, which avoids the fee imposition only upon recording the

content data on the optical disk 1601. Accordingly, it becomes possible to lower the imposed fee,

(a) for the users who wish to listen and watch content, but do not need to record content data on the optical disk 1601, or
(b) for the users who wish to record content data on the optical disk 1601; but do not need to listen and watch content upon broadcasting,

as compared with the case in which a fee is imposed once for both listening or watching and recording on the optical disk 1601.

**[0130]** Also, since a fee is not imposed for only recording on the optical disk 1601, the user can determine whether or not the user receives the key for reproducing the optical disk 1601 to listen and watch again after listening and watching. Although, in the above-mentioned preferred embodiment, a method for receiving the key (DK) from the control section 1701a of the key issuing center apparatus 1707 via the network is used, the present invention is not limited to this, the title and the disk ID number of the content may be orally conveyed on the phone or the like, and be inputted using a keyboard after being received orally.

**[0131]** Next, the case will be described where the optical disk 1601, on which the key (DK) is recorded in the key information recording area 1605, is reproduced after access to the key issuing center apparatus 1707 is completed. First of all, a laser beam outputted from the optical pickup is irradiated onto the area of the optical disk 1601 where the above-mentioned content is recorded, and then, the reflected light is inputted to the data reproducing section 1721 via the optical pickup which carries out the photoelectric conversion. In response to this, the data reproducing section 1721 outputs the data of the encrypted content to the second cipher decoder 1722. On the other hand, a laser beam outputted from the optical pickup is irradiated onto the BCA 1604 of the optical disk 1601 so that the reflected light is inputted into the BCA reproducing circuit 1720 via the optical pickup which carries out the photoelectric conversion. In response to this, the BCA reproducing circuit 1720 generates the disk ID signal 1715 based on the inputted reproduced signal, which is outputted to the second cipher decoder 1722.

**[0132]** In addition, the laser beam outputted from the optical pickup is irradiated onto the key information recording area 1605 of the optical disk 1601 so that the reflected light is inputted into the key information reproducing section 1723 via the optical pickup which carries out the photoelectric conversion. In response to this, the key information reproducing section 1723 generates data of the key (DK) based on the inputted reproduced signal, which is outputted to the second cipher decoder 1722. The second cipher decoder 1722 decrypts the encrypted content outputted from the data reproducing section 1721, using the decipher key including the inputted disk ID signal 1715, the key (DK) and the title code 1716 of the above-mentioned content. The decoding process of the second cipher decoder 1722 is expressed in the following equation. When the content is an image signal, an MPEG signal is, for example, expanded, and the image signal of the expanded MPEG signal is outputted from the second cipher decoder 1722.

$$C\,[FK]\,\#\,(DK * BCA * T) = C\,[FK]\,\#\,FK = C \quad (15)$$

**[0133]** By recording the data of the key (DK) once in the key information recording area 1605, the above-mentioned encrypted content can always be reproduced without any access to the key issuing center apparatus 1707. Also, since all of the decipher keys required for the decrypting process are recorded on the optical disk 1601, the above-mentioned optical disk 1601 can be reproduced by an arbitrary optical disk recording and reproducing apparatus comprising the BCA reproducing circuit 1720, the key information reproducing section 1723 and the second cipher decoder 1722.

**[0134]** In addition, in the case that the above-mentioned encrypted content is attempted to be reproduced after being copied onto the optical disk 1601 with a different disk ID, a disk ID signal different from that of the above-mentioned optical disk 1601 is outputted from the BCA reproducing circuit 1720, therefore, the encrypted content cannot be decrypted, and this prevents the content from being reproduced after being copied. Even in this case, however, by conveying the title and the disk ID of the content to the key issuing center through the network or orally, the decipher key may be received after the fee is imposed. In this way, even if the encrypted content is copied onto another optical disk 1601, any content cannot be reproduced irregularly, and a fee is always imposed when the optical disk 1601 on which the encrypted content is copied, is reproduced, and this leads to protection of copyright for the content.

**[0135]** Fig. 23 shows a table showing a configuration of the table with IDs according to the fifth preferred embodiment, which shows keys (K) inputted into the first cipher decoder 1713 and keys (DK) inputted into the key information recording circuit 1719 in a rearranged form, for different system IDs and different disk IDs.

**[0136]** Referring to Fig. 23, T1, T2 and T3 denote title codes for different contents, and FK1, FK2 and FK3 denote decipher keys for decoding encrypted contents having the title codes of T1, T2 and T3, respectively. DID1, DID2 and DID3 denote system IDs for different CATV decoders 1706, and BCAS1, BCAS2 BCAS3 denote disk IDs for different optical disks 1601. In this case, keys (Kmn) inputted into the CATV decoder 1706 are

determined so as to satisfy the following equation:

$$FKn = Kmn * Tn * DID * TIMEn \quad (16).$$

**[0137]** Also, the keys (DKmn) inputted to the optical disk recording and reproducing apparatus 1714 are determined so as to satisfy the following equation:

$$FKn = DKmn * BCAm * Tn \quad (17).$$

**[0138]** As shown in Fig. 23, not only in the case of different content but also in the case of the same content, the key information acquired from the key issuing center apparatus 1707 for each different CATV decoder 1706, for each different optical disk and for each different broadcasting time is set so as to be different from each other, and then, this leads to protection of copyright in detail. In the same way, since the key information differs when the system IDs, disk IDs and time information are different from the others even for the same content, it is not necessary for the CATV company apparatus 1701 to change the encrypted content for each user, therefore, one encrypted content may be prepared for one content. Therefore, the system for broadcasting can be simplified, and it becomes possible to supply the content to a mass audience at low cost.

**[0139]** Although, in the present preferred embodiment, the case described where the content is broadcasted from a head end of the cable television, the present invention can be applied to broadcasting using radio wave.

## ADVANTAGEOUS EFFECTS OF THIRD TO FIFTH PREFERRED EMBODIMENTS

**[0140]** An optical disk according to the present preferred embodiment comprises (a) a first information area for recording first disk information therein, (b) a second information area for recording therein second disk information for identifying individual, and (c) a user data area in which recording information is possible by irradiating a light beam onto the user data area. Accordingly, by adding the above-mentioned information for identifying optical disks to an optical disk according to a prior art, the management of optical disks can be easily implemented. In this case, the above second information area is preferably recorded in the above-mentioned first information area, and can be reproduced by the optical pickup for reproducing the above-mentioned first information area. In the above-mentioned second information area, data of the second information is recorded by partially eliminating or removing the recording film within the above-mentioned first information area so that a plurality of trimming areas having an elongated shape in the radius direction are formed, and this can prevent the above-mentioned second disk information from being easily falsified.

**[0141]** According to a method for recording encrypted content of the present preferred embodiment, when the data of the content is recorded on the user data area of an optical disk comprising (a) a first information area for recording the first disk information therein, (b) a second information area for recording therein the second disk information for identifying individual disks, and (c) a user data area in which recording information is recorded by irradiating a light beam onto the user data area, the data of the content is encrypted and the encrypted data is recorded so that the data of the content can be decrypted and reproduced by an operation or calculation using at least the above-mentioned second disk information. Accordingly, by encrypting the content using the identification information of an optical disk which exists only in one particular optical disk, there is such a specific advantageous effect that irregular copying of the content can be prevented so as to protect the copyright.

**[0142]** An optical disk according to the present preferred embodiment has a key information recording area for recording therein key information for decrypting encrypted and recorded content within the user data area. Accordingly, in a system which needs key information for decrypting the encrypted and recorded content, there is such a specific advantageous effect that it is not necessary to input key information every time of reproduction after recording the key information once in the key information recording area.

**[0143]** Furthermore, according to a method for recording encrypted content of the present preferred embodiment, when the content is recorded in the user data area of an optical disk comprising (a) a first information area for recording the first disk information therein, (b) a second information area for recording therein the second disk information for identifying individual disks, (c) a user data area in which information is recorded by irradiating a light beam onto the user data area, and (d) a key information recording area for recording therein key information for decrypting the data of the encrypted and recorded content within the user data area, the data of the content is encrypted and the encrypted content is recorded so that the data of the content can be decrypted and reproduced by the operation using at least the above-mentioned second disk information and the above-mentioned key information. Accordingly, even if the data of the encrypted content are copied onto another optical disk, the data thereof cannot be reproduced irregularly, and a fee is always imposed whenever the optical disk on which the data of the encrypted content are copied is reproduced, and this leads to protection of copyright.

**[0144]** In this case, the first disk information is preferably formed in a form of micro concavo-convex pits, and the second disk information for identifying optical disks is recorded on the concavo-convex pits. Therefore, the second disk information can be easily prevented from being falsified. Moreover, said first disk information and

the second disk information are preferably formed to be adjacent from each other. In this case, when the above-mentioned first disk information is reproduced, the second disk information can be reproduced continuously, or when the second disk information is reproduced the first disk information can be reproduced continuously, therefore, it becomes possible to accelerate the process for recording the encrypted content after obtaining or acquiring the second disk information for identifying disks quickly by a CPU when, for example, the optical disk is started up.

**[0145]** According to a method for recording encrypted data of the present preferred embodiment, since key information differs for each different system ID, each disk ID and each time information even with the same content, it is not necessary for the CATV company apparatus 701 to change the encrypted content for each user, and then, the CATV company apparatus 701 may only prepare one encrypted content for one content. This leads to that the system for broadcasting can be simplified, and it becomes possible to supply the content to a mass audience at low cost.

## MODIFIED PREFERRED EMBODIMENTS OF THIRD AND FIFTH PREFERRED EMBODIMENTS

**[0146]** Although in the above-mentioned third and fifth preferred embodiments, as shown in Figs. 16 and 21, trimming areas 1105 and 1606 are formed in the BCAs 1104 and 1604 located in the inner periphery section within the control user data areas 1102 and 1602 respectively, the present invention is not limited to this. As shown in Figs. 24 and 25 illustrating the data recording areas of the optical disks 1101a and 1601a according to the modified preferred embodiments of the third and the fifth preferred embodiments respectively, the trimming areas 1105a and 1606a may be formed by trimming the recording film so as to protrude or project into the inner peripheral side of the optical disk from the control user data areas 1102 and 1602. That is to say, the BCAs 1104a and 1604a are not included in the control user data areas 1102 and 1602, respectively, but are formed and allocated so as to protrude or project into the inner side of the control user data areas 1102 and 1602 from the inner peripheral section of the control user data areas 1102 and 1602. In these modified preferred embodiments, the reason why the BCAs 1104a and 1604a are formed in this way is that the margin is taken into consideration where the diameter of the beam spot of the laser beam fluctuates due to the instability of the focusing servo circuit of the laser device. In the present modified preferred embodiment, the user data areas 1103 and 1603 exist outside of the control user data areas 1102 and 1602, therefore, the trimming areas 1105a and 1606a are allocated and formed so as to protect the data recorded in those user data areas 1103 and 1602 from being destroyed.

## SIXTH PREFERRED EMBODIMENT

**[0147]** Fig. 26 shows a block diagram illustrating a configuration of a user data area within an optical disk and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data in the user data area, according to a sixth preferred embodiment of the present invention. In the present preferred embodiment, the optical disk is, for example, a recording-type optical disk such as a DVD-RAM.

**[0148]** As shown in Fig. 26, a user data area 2150 comprises a sector header area 2101, a main data area 2102, and an error detection code 2103. In the sector header area 2101, a sector address 2104 for indicating a sector position, and copyright control information 2105 for recording the copyright control information (including a scramble flag, copy control information or the like) with respect to the data recorded in the main data area 2102 are recorded. The sector head area 2101 includes a decipher key area 2106 for decrypting encryption information when it has been embedded or encrypted in the data of the main data area 2102. Also, the main data area 2102 are divided into an area in which non-encrypted content 2107 is recorded and an area in which the encrypted content 2108 is recorded, and the non-encrypted content 2107 includes control information for subsequent data such as synchronizing patterns in the MPEG or all types of control information. In addition, the encrypted content 2108 includes content data required for copyright protection primarily such as AV data or the like which have been encrypted.

**[0149]** The decipher key for reproducing the following main data area 2102 is divided into a plurality of divided decipher keys with a predetermined size (hereinafter referred to as divided decipher keys), which are then registered in the decipher key area 2106. For example, in the case that the decipher key is 8 bytes for one decipher key area of 4 bytes, the decipher key of 8 bytes is divided into two divided decipher keys each of 4 bytes, so that the two divided decipher keys are recorded in decipher key areas 2106 and 2109 of two logically continuous sectors after dividing the decipher key of 8 bytes into divided decipher keys each of 4 bytes. When reproducing data of such a user data area, a plurality of divided decipher keys are acquired from the decipher key areas 2106 and 2109 of the logically continuous plurality of sectors (each sector which is not available due to defects is skipped), and the acquired divided decipher keys of the required number are linked or connected by a data linking device 2111 to obtain the encrypted decipher key required for the reproduction (8 bytes). A decrypting process is carried out for the data recorded in the main data area 2102 of the sector where the encrypted decipher keys (B bytes) could be obtained by a decrypting device 2114 in accordance with the contents of each unit of copyright control information 2105.

**[0150]** In addition, to further enhance the intensity of the encryption it is possible to encrypt the decipher key,

or by adding the decipher key conversion data which is the information in the data to the key so as not to have a constant result of the encryption, it becomes possible to provide different encryption results even for the same cipher key. More concretely, as shown in Fig. 26, the encrypted decipher key outputted from the data linking device 2111 is inputted to the key decrypting device 2112, and then, using a predetermined disk key, the key decrypting device 2112 decrypts the inputted encrypted decipher key into the padding data (1 byte) which are dummy data and the decipher key (7 bytes), which are then outputted to the key converter 2113. In this case, the disk key is acquired by decrypting, for example, an encrypted disk key recorded in the optical disk using a secret key which is a predetermined master key by the disk key decrypting device (not shown). Also, the key converter 2113 converts data of the decipher key conversion data 2110 read out from the main data area 2102 through a predetermined conversion operation such as an operation utilizing multiplication, division or predetermined weighting coefficients by using the decipher key outputted from the above-mentioned key decrypting device 2112, and then, generates and outputs a content decipher key (7 bytes) to the decrypting device 2114. Then, the decrypting device 2114 generates and outputs the data of the decrypted content by decrypting the data of the content read out from the main data area 2102 using the content decipher key (7 bytes) outputted from the above-mentioned key converter 2113. As the decipher key conversion data 2110, it is preferable to utilize the data such as data that the irregular usage of the data such as falsifying the copy generation management information or the analog macro-vision control flag can be immediately detected.

**[0151]** Fig. 27 is a block diagram showing an arrangement of the copyright control information and the decipher key in the user data area and an allocation of the encrypted content in the main data area of an optical disk, according to the sixth preferred embodiment. In an example of the user data area 2150 illustrated in Fig. 27, the decipher key area is arranged so as to be divided into the first decipher key area 2201 having a division decipher key of 4 bytes and the second decipher key area 2202 having a division decipher key of 4 bytes. Therefore, in spite of the size of the encrypted content recorded in those two sectors, a plurality of sectors (2 sectors in Fig. 27) are utilized. In this case, dummy data is recorded in the unused area as complementary data. In an example of Fig. 27, complementary data 2203 for one sector is recorded in the case that the encrypted content 2204 exits only for one sector.

**[0152]** Fig. 28 is a block diagram showing an arrangement of the case where the unit of error correction is located over a plurality of sectors in an optical disk according to the sixth preferred embodiment. For example, in the case that the optical disk is a DVD, the ability of error correction is enhanced by using a unit block (hereinafter referred to an ECC block) of error correction code of 16 sectors. Therefore, when data recording or reproducing is carried out, it is necessary to perform the recording process using the ECC block unit. In the case that the decipher key is divided into an arbitrary number of divided decipher keys which are then recorded, the case may be caused where one decipher key is recorded in a plurality of error correction blocks. When reproducing the same, it is necessary to reproduce all of the plurality of divided decipher keys, therefore, it is also necessary to reproduce not only data in the sector for recording the data of the encrypted content but also data in the ECC block immediately before decipher key is recorded. An example of Fig. 28 is characterized in that the number of divisions when the decipher key is divided is set as a measure or factor of the number of sectors of the ECC blocks. This leads to that a plurality of divided decipher keys cannot be recorded so as to located over a plurality of ECC blocks. In addition, as a decipher key used in one ECC block, only one type of decipher key is used, and in the case that the recorded AV data are not sufficient for an ECC block, the data of the sectors which are unnecessary upon reproduction can be prevented from being read out from the optical disk by arranging complementary data and complementary sectors.

## SEVENTH PREFERRED EMBODIMENT

**[0153]** Fig. 29 is a block diagram showing a configuration of a lead-in area 2401 and a user data area 2402 within an optical disk and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from data of the lead-in area 2401 and the user data area 2402, according to the seventh preferred embodiment of the present invention.

**[0154]** Referring to Fig. 29, in the same way as in that of the sixth preferred embodiment of Fig. 26, each of the lead-in area 2401 and the user data area 2402 is constructed from sectors having a sector header area 2101, the main data area 2102 and an error detection code 2103. In the sector header area 2101, there are recorded a sector address 2104 for indicating the position of the sector and copyright control information 2105 for recording copyright control information (including a scramble flag, copy control information or the like) with respect to the data recorded in the main data area 2102, and also the sector header area 2101 includes a key index area 2403 for recording a key index for indicating the recording position of the decipher key (that is, the recording position of storing position in a decipher key table 2404 within the main data area 2102) for referring to a decipher key for decrypting in the case that the data of the main data area 2102 are encrypted. The decipher key for decrypting the encrypted content recorded in the user data area 2402 is recorded in a form of a decipher key table 2404 in the lead-in area 2401 which is rewritable in a form of a table. The decipher key recorded in the lead-in area 2401 is referred to by the key index re-

corded in the key index area 2403. In the same way as that of the sixth preferred embodiment illustrated in Fig. 26, the decipher key referred to in the above is decrypted into the padding data and the decipher key (or title key) by the key decrypting device 2112 using a predetermined disk key, and thereafter, the above decrypted decipher key (or title key) is converted into a content decipher key by the key converter 2113 using the decipher key conversion data, and then, the converted content decipher key is outputted to the decrypting device 2114. The decrypting device 2114 decrypts the data of the encrypted content by using the content decipher key, and then, generates and outputs data of the decrypted content.

**[0155]** In an optical disk and an optical disk reproducing apparatus according to the seventh preferred embodiment constituted as described above, by recording a key index for reference in the key index area 2403 within the sector header area 2101, it becomes possible to allocate the decipher key size of the decipher key table 2404 independently from the size of the key index area 2403. Also, after allocating the size of the decipher key table 2404, by utilizing a plurality of decipher keys continuously from the decipher key table 2404 indicated by the key index within the key index area 2403, a decipher key of an arbitrary or free size can be used.

**[0156]** Fig. 30A is a block diagram showing a data configuration of the case where an initial value of a decipher key represents an unrecorded status in the main data area 2102 of the lead-in area 2401 within an optical disk according to the seventh preferred embodiment. Referring to Fig. 30A, as the initial value of the decipher key recorded upon formatting of the optical disk or the like, the data in the unrecorded status 2501 is recorded with an already known fixed value (for example, data such as all zeros) which are not used as a key, thereby to indicate the unrecorded status of the decipher key.

**[0157]** Fig. 30B is a block diagram showing a data configuration of the case where a recorded status is represented with a decipher key status table in the main data area 2102 of the lead-in area 2401 within an optical disk according to the seventh preferred embodiment. Referring to Fig. 30B, in the same way as that of the decipher key illustrated in Fig. 30A, the decipher key status table 2502 in a form of table which can be referenced by an index is arranged in the lead-in area 2401, and the recorded status of the decipher key is described as follows as record status data 2503:

(1) 0x00: unused;
(2) 0x01: area reservation;
(3) 0x03: key recorded; and
(4) otherwise: reserved.

**[0158]** In this case, 0x indicates a hexadecimal representation of the following symbols or numbers.

**[0159]** Fig. 31 is a block diagram showing an allocation of decipher keys in an optical disk according to the seventh preferred embodiment. In an example of Fig. 31, an allocation of the decipher key area of the disk is devised to enhance the reliability of the decipher keys. Usually, defect management is carried out in the user data area 2602, and therefore, in the case that a write failure occurs, a replacement process for an area to be replaced or the like is carried out. In the lead-in area 2601, however, the defect management as described above is not carried out. Therefore, by occurrence of write-in failure, read-out failure or the like, the decipher key, which is required for producing the AV data, may be converted into an unusable status, and moreover, there may be the case the optical disk itself may be converted into an unusable status. Accordingly, a total plurality of decipher keys are desired to be recorded over a plurality of different ECC blocks. In the case that a plurality of decipher keys is recorded in areas adj acent from each other, all of the entire plurality of decipher keys which has been recorded may not be read out due to scratches or dust. Therefore, as shown in Fig. 31, it is preferable to record in separate positions in a layout, such as the inner peripheral side and the outer peripheral side of the optical disk, respectively, for example, in the lead-in area 2601 and the lead-out area 2603.

**[0160]** In the preferred embodiment of Fig. 29, the decipher key areas are allocated in the lead-in areas 2401 and 2601. This is because to enhance the safety when access is taking place from a drive unit of a personal computer or the like, with taking into consideration that the user data area 2602 is an accessible area by a conventional read command or write command. Accordingly, the same advantageous effects can be obtained by allocating these in the user data area 2602.

## EIGHTH PREFERRED EMBODIMENT

**[0161]** Fig. 32 is a block diagram showing a data configuration when data of an optical disk is managed by a file management system of an eighth preferred embodiment according to the present invention. In an example of Fig. 32, based on a structure of the file system, a sector address for storing a desired file is managed.

**[0162]** In the structure of a file system prescribed or regulated in the ISO 13346 by the International Standardization Organization, a recording position of a file is managed by using the information called a file entry in order to utilize a rewritable-type optical disk. As shown in Fig. 32, for example, data of a recording position of a file (1) 2703 is stored as a file entry (1) 2701 within a file management information area 2751, and data of a recording position of a file (2) 2704 is stored as a file entry (2) 2702. Each file is constituted from extents 2705 and 2706 for managing a plurality of sector areas which are located so as to continue on the optical disk. The encrypted content as shown in the seventh preferred embodiment is recorded in the main data area 2102 indicated by the file entry on the optical disk, and the decipher key is recorded in the decipher key table 2707 with-

in the lead-in area 2601. In the sector header area 2101 within the user data area 2602 where the encrypted content is recorded, a pointer for indicating a recording position for referring to a decipher key required for decrypting is recorded in the key index area 2708. Although, in the present preferred embodiment, the decipher key is managed and recorded using the file unit, the extent unit, the present invention is not limited to this. The decipher key may be managed and recorded using at least one of either of the file unit or the extent unit.

**[0163]** As described above in the optical disk, managed by the file system, the recording operation of the content required for copyright protection will be described with reference to Fig. 33. Fig. 33 shows a recording process of a content required for copyright protection carried out by a file management system according to the eighth preferred embodiment.

**[0164]** When recording the encrypted content, first of all, in step S2801, the decipher key status table 2502 illustrated in Fig. 30B is read out to check empty areas of the decipher key table 2707. Next, in step S2802, it is determined whether or not there is any empty area of the decipher key table 2702, and in the case of NO, the recording process of the content is completed by stopping the recording operation in step S2807 because the decipher key for the encrypted content cannot be recorded. On the other hand, in the case of YES in step S2802, the acquired decipher key (or the title key) is recorded, and in the case that the decipher key cannot be acquired, the decipher key area is reserved. Next, in step S2804, the copyright control information of the recorded content (including information about whether or not encryption has been performed, information for indicating the type or class of encryption or the like) and the key index to be recorded in the key index area 2708 are set, and thereafter, the content is encrypted in step S2805 and then the encrypted content is recorded on the optical disk in a file form using the extent unit. In this case, the same copyright control information and key index may be used utilizing the file unit or they may be switched utilizing the extent unit. That is to say, in steps S2804 and S2805, the unit to be processed is at least one of either the file unit or the extent unit. Finally, in step S2806, based on the information with respect to the recorded content, after the file management information for managing the above-mentioned recorded data is updated, the recording process of the content is completed.

**[0165]** Fig. 34 is a flowchart showing a reproducing process of content carried out by a file management system according to the eighth preferred embodiment. Fig. 34 shows a process for reproducing the content recorded in a form of file from the optical disk by the method shown in Fig. 33.

**[0166]** When carrying out a reproducing operation for the file, the key index is acquired for the areas shown by the file entry within the file management information area 2751 in order to find out or know the area in the decipher key table utilized by the reproduced file. More concretely, in step S2901, after the file entry of the file reproduced from the file management information 2751 is acquired by being read out and reproduced, in step S2902 the value of the key index area is read out, and then reproduced from the sector header area 2102 of the area shown by the file entry to be acquired. In the case that different ways of encrypting are used are conducted utilizing the extent unit, the key index area in the sector header for each extent is read out. Then, in step S2903, the decipher key is read out, and then reproduced to acquire the decipher key from the decipher key area of the decipher key table 2707 indicated by the acquired key index. In addition, in step 52904, the data of the content within the file is read out and reproduced from an area shown by the file entry, and then, data of the reproduced content is decrypted. In this case, when reproduction and the decrypting of the file of the content are completed, the reproducing process of the content is completed.

**[0167]** Fig. 35 is a flowchart showing an deleting process of content which is carried out by the file management system according to the eighth preferred embodiment, and Fig. 35 shows an operation for deletion of data of content in a form of file which has been recorded by the method as shown in Fig. 33.

**[0168]** When the deleting operation of the file is carried out, the key index for the area shown by the file entry is acquired to find out or know the areas of the decipher key table 2707 used by the deleted file. More concretely, in step S3001, after acquiring the file entry of the deleted file from the file management information within the file management information area 2751, in step S3002 the value of the key index area is acquired from the sector header of an area indicated by the file entry is acquired. In this case, when different ways of encrypting are conducted utilizing the extent unit, data in the key index area in the sector header for each extent is read out. Then, in step S3003, after the decipher key is open or released (here releasing or opening the decipher key means to delete the decipher key from the table) from the decipher key area of the decipher key table 2707 indicated by the acquired key index, and in step S3004 the file entry for indicating the write-in position of the deleted file is deleted from the file management information, then, the deleting process of the content is completed. Although in a conventional file system only the file entry is deleted when the file is deleted, the decipher key recorded in another area cannot be deleted since the decipher key and the record sector of the encrypted content are recorded in separate areas. In the above-mentioned preferred embodiments, prior to deletion of the file entry, the management of the decipher key on the optical disk is carried out by deleting the decipher key for indicating the key index in the sector header area, from the decipher key table 2707.

NINTH PREFERRED EMBODIMENT

**[0169]** Fig. 36 is a block diagram showing a configuration of an optical disk system of a ninth preferred embodiment according to the present invention, and this optical disk system is a information processing system for recording and reproducing content required for copyright protection for the optical disk 3100. The optical disk system comprises an encoding apparatus 3101, an optical disk apparatus 3102, a decoding apparatus 3103 and a personal computer 3104.

**[0170]** The encoding apparatus 3101 comprises a content memory 3131 for storing data of content, an encoding circuit 3132 for encoding the above-mentioned data of the content in a form of MPEG format, a cipher key memory 3133 for storing the cipher key, an encrypting circuit 3134 for encrypting the data of the encoded content utilizing the cipher key and generating and storing the decipher key in the decipher key memory 3111, a decipher key memory 3111 for storing the decipher key, a bus encryption circuit 3112 for bus-encrypting the decipher key, and an interface 3124 connected to the interface 3122 of the personal computer 3104 via a PCI bus 3151, where the interface 3124 transmits the data of the encrypted content and the decipher key. Also, the optical disk apparatus 3102 comprises a decipher key table memory 3113 for storing a plurality of decipher keys therein, a bus encrypting and decrypting circuit 3114, a recording and reproducing circuit 3119 for recording the data onto the optical disk 3100 and for reading out and reproducing the data from the optical disk 3100, and an interface 3120 connected to the interface 3121 of the personal computer 3104 via a SCSI bus 3152, where the interface 3120 carries out processes such as transmission and reception of data or signals as well as signal conversion and protocol conversion. The SCSI bus 3152 may be preferably an ATAPI bus. In this case, bus encryption and bus decryption mean the cipher process and the decipher process, respectively, used for encrypting a cipher key or a decipher key and transmitting or receiving the same key on the PCI bus 3151 or the SCSI bus 3152.

**[0171]** In addition, the personal computer 3104 comprises a control section 3130 for controlling the operation of the personal computer 3104, a bus encryption decipher key table memory 3115 for storing a plurality of bus encryption decipher keys therein, a decipher key status table memory 3116 for storing data of a plurality of decipher key statuses (indicating a recording status or condition of a plurality of decipher key status, more concretely indicating non-usage or unused, area reservation, key recorded, reserved or the like) corresponding to the above-mentioned plurality of bus encryption decipher keys, an interface 3121 connected to the interface 3120 or the optical disk apparatus 3102 via the SCSI bus 3152 where the interface 3121 carries out processes such as transmission and reception of the data and the signals as well as signal conversion and protocol conversion, and an interface 3122 connected to the interface 3123 of the decoding apparatus 3103 and the interface 3124 of the encoding apparatus 3101 via the PCI bus 3151 where the interface 3122 carries out processes such as transmission and reception of the data or the signals as well as signal conversion and protocol conversion. In addition, the decoding apparatus 3103 comprises an interface 3123 connected to the interface 3122 of the personal computer 3104 where the interface 3123 carries out processes such as the transmission and the reception of the data or the signals as well as signal conversion and protocol conversion, a bus decrypting circuit 3117 for bus-decrypting or bus-decoding the encryption decipher key received by the interface 3123, a decipher key memory 3118 for storing the decipher key therein, and a decryption circuit 3141 for decrypting or coding the data of the encrypted content received by the interface 3123 using the decipher key of the decipher key memory 3118 as well as generating an image signal or a speech sound signal by carrying out the decoding process of the MPEG format, where the generated image signal and speech sound signal are outputted to a display apparatus 3105.

**[0172]** In the encoding apparatus 3101 of this optical disk system, the encoding circuit 3132 encodes the data of the content such as the AV data stored or inputted to the content memory 3131 in a form of MPEG format, and the encrypting circuit 3134 encrypts the data of the above encoded content using the cipher key within the encrypting key memory 3133 which is generated to avoid an irregular usage of the content on a personal computer 3104, and then, and transmits the data of the encoded content to the optical disk apparatus 3102 via the interface 3124 and the personal computer 3104. In this case, the data of the encrypted content is transmitted to the recording and reproducing circuit 3119 via the PCI bus 3151, the interface 3122 and the interface 3121 of the personal computer 3104 and the interface 3120 of the optical disk apparatus 3102 from the interface 3124 of the encoding apparatus 3101. Then the data of the encrypted content is recorded on the optical disk 3100 by the recording and reproducing circuit 3119 of the optical disk apparatus 3102. Also, the recording and reproducing circuit 3119 of the optical disk apparatus 3102 reproduces the data of the encrypted content recorded on the optical disk 3100, and then, transmits the data of the reproduced encrypted content to the decrypting circuit 3141 via the interface 3120, the interface 3121 and the interface 3122 of the personal computer 3104 and the interface 3123 of the decoding apparatus 3103. The decrypting circuit 3141 of the decoding apparatus 3103 decrypts the encryption for the data of the encrypted content, and carries out a decoding process of MPEG format, then outputs an image signal or a speech sound signal of the decoded content to a display apparatus 3105 and a speaker apparatus (not shown), respectively.

**[0173]** The encryption circuit 3134 of the encoding ap-

paratus 3101 carries out the encryption for the data of the encoded content in a form of MPEG format using the cipher key within the cipher key memory 3133, and at the same time, generates and stores the decipher key required upon reproduction in the decipher key memory 3111. Although it is necessary to record the data of the encoded content and the decipher key on the optical disk 3100, in the case that the decipher key is handled as plain text on the personal computer 3104, there is such a possibility that the decoding of the data of the encrypted content may become easy by reading out the decipher key from the optical disk 3100. In order to avoid this mutual authorization is carried out between the encoding apparatus 3101 and the optical disk apparatus 3102 and a bus encryption is carried out using a bus key mutually shared.

**[0174]** That is to say, more concretely, the decipher key stored in the decipher key memory 3111 is encrypted by a bus encryption circuit 3112 of the encoding apparatus 3101, and thereafter, the encrypted decipher key is stored in a bus encryption decipher key table memory 3115 of the personal computer 3104 via the interface 3124, the PCI bus 3151 and the interface 3122. On the other hand, in the bus encrypting and decrypting circuit 3114 of the optical disk apparatus 3102, the decoding of the encrypted decipher key which is reproduced by the recording and reproducing circuit 3119 from the optical disk 3100 is carried out, and thereafter, the decipher key which has been decrypted or decoded is stored in a decipher key table memory 3113. Also, the bus encrypting and decrypting circuit 3114 receives and bus-decrypts, for example, the updated and bus-encrypted decipher key via the interface 3121, the SCSI bus 3152 and the interface 3120 from the bus encryption decipher key table memory 3115, and stores the bus-decrypted decipher key in the decipher key table memory 3113. Thereafter, the bus-decrypted decipher key is recorded on the optical disk 3100 by the recording and reproducing circuit 3119.

**[0175]** After the decipher key status table is reproduced from the optical disk 3100 by the recording and reproducing circuit 3119, the decipher key status table is transferred to and stored in the decipher key status table memory 3116 via the interface 3120, the SCSI bus 3152 and the interface 3121. In addition, the decipher key status table updated by the personal computer 3104 is read out from the decipher key status table memory 3116, and then, is transferred to the recording and reproducing circuit 3119 via the interface 3121, the SCSI bus 3152 and the interface 3120. Thereafter, the recording and reproduced circuit 3119 records the received decipher key status table on the optical disk 3100. Accordingly, only the encrypted decipher key is handled on the personal computer 3104, which is located in the middle, by using the encryption decipher key table 3115 and the decipher key status table memory 3116, and this leads to establishment of more security.

**[0176]** Carrying out a bus-encryption of the decipher key in the same way between the optical disk apparatus 3102 and the decoding apparatus 3103 leads to establishment of more security. That is to say, the bus decrypting circuit 3117 of the decoding apparatus 3103 bus-decrypts or bus-decodes the encrypted decipher key received from the personal computer 3104 via the interface 3123, and stores the bus-decrypted decipher key in the decipher key memory 3118. The decrypting circuit 3141 decrypts the data of the encrypted content using the decipher key stored in the decipher key memory 3118.

**[0177]** As shown in the above-mentioned seventh preferred embodiment, in the case that the decipher key for decrypting the data of the encrypted content on the optical disk 3100 is recorded in a form of table, the decipher key table reproduced by the optical disk apparatus 3102 is bus-encrypted by the bus encrypting and decrypting circuit 3114, and thereafter, the data of the bus encrypted decipher key table is transferred to the bus encrypted decipher key table memory 3115 of the personal computer 3104 via the interface 3120, and is stored therein. When the data of the content is recorded, the personal computer 3104 searches by retrieving an empty area of the decipher key table from the decipher key status table recorded in the optical disk 3100 in a form of plain text, and then, the bus encrypted decipher key transferred from the encoding apparatus 3101 is allocated to the searched empty area. In this case, when such an encryption as completing with the decipher key unit as a bus encryption (for example, a block encryption with a unit of decipher key length), it is not necessary to decrypt and re-encrypt the decipher key upon allocation thereof to the decipher key block.

**[0178]** Since the decipher key table and the decipher key status table transferred and stored among the optical disk apparatus 3100, the optical disk apparatus 3102 and the personal computer 3104 are one piece of block data, respectively, they can be called a block data.

**[0179]** In the case when the content is reproduced, only the decipher key required for decrypting of the content desired to be reproduced from the decipher key block reproduced from the optical disk apparatus 3102 is retrieved and taken out from the bus encrypted decipher key table memory 3115, and the taken decipher key is transferred to and stored in the decipher key memory 3118 via the bus decrypting circuit 3117 of the personal computer 3104 and the decoding apparatus 3103. Then the decrypting circuit 3141 receives encrypted AV data reproduced from the optical disk 3100 by the recording and reproducing circuit 3119 of the optical disk apparatus 3102 via the personal computer 3104 and the interface 3123, and thereafter, the received encrypted AV data is decrypted using the decipher key within the decipher key memory 3118, and the decrypted data is outputted as an image signal and a speech sound signal In this case, in a manner similar to that of above described case, when the content is recorded, it is not necessary to decrypt and re-encrypt the decipher key when

the decipher key is taken out from the decipher key block when such an encryption as completing with a unit of decipher key as a bus encryption (for example, a block encryption with a unit of decipher key length). Furthermore, when the size of the decipher key is enlarged, the expansion of the decipher key area such as allocating a plurality of decipher keys can be carried out easily and safely on the personal computer 3104 without changing any configuration of the optical disk apparatus 3102.

TENTH PREFERRED EMBODIMENT

**[0180]** Fig. 37 is a block diagram showing a configuration of a user data area on an optical disk, a configuration of an optical disk recording apparatus for encrypting content and recording encrypted content in the user data area, and a configuration of an optical reproducing apparatus for decrypting an encrypted content from data in the user data area, according to a tenth preferred embodiment of the present invention. This tenth preferred embodiment is characterized in that the configuration of the optical disk recording apparatus is added to that of the sixth preferred embodiment, and the configuration thereof will be described in detail.

**[0181]** In the optical disk recording apparatus, in order to enhance the intensity of the encryption so as not to have a constant encryption result, after obtaining or acquiring a content decipher key by performing a predetermined key conversion on the inputted cipher key such as multiplication, division or an operation (calculation), using a predetermined weighting coefficient by the key converter 2119 using the decipher key conversion data which is the information in the content, the data of the content is encrypted by using the content decipher key

**[0182]** That is to say, when the content is recorded, the data of the content and the cipher key for encrypting the data of the content are inputted to the optical disk recording apparatus. In this case, the data of the content are inputted to the key converter 2119 and the encrypting device 2120, and the cipher key is inputted to the key encrypting device 2118 and the key converter 2119. The key converter 2119 performs an operation or calculation of a predetermined key conversion on the above-mentioned inputted cipher key, using the first and the second decipher key conversion data 2115 and 2116, which are respectively part of the information in the content, and then, generates and outputs a content decipher key to the encrypting device 2120. Then the encrypting device 2120 encrypts the data of the above-mentioned inputted content using the above-mentioned content decipher key, and then, records the encrypted content in an AV data recording sector 2152 within the user data area 2150 on the optical disk.

**[0183]** In this case, as the decipher key conversion data used in the optical disk reproducing apparatus are utilized, the second decipher key conversion data 2116, which is the information in the AV data and which is generally different in a unit of sector, copy generation management information included in the sector in which control information is recorded, and the first decipher key conversion data 2115 which is copy control information including an analog macro-vision control flag. By utilizing the former second decipher key conversion data, it becomes possible to recover the content decipher key for encrypting the data of the content for each sector by the key converter 2113 in accordance with the content of the second decipher key conversion data. Also, since the latter first decipher key conversion data is data for which irregular utilization can be easily detected upon falsification, such an advantageous effect can be obtained that it can readily be possible to prevent the data of the content from being decrypted when the first decipher key conversion data is falsified. More concretely, the cipher key is converted into a decipher key though a predetermined conversion operation using the data in the reproduction control recording sector for recording reproduction control information used for reproduction control of the AV data as the first decipher key conversion data, and the converted decipher key is used as a content decipher key in the encrypting device 2120. In addition, by performing a predetermined conversion operation or calculation on the cipher key using the two pieces of decipher key conversion data including the first decipher key conversion data, which is data in the reproduction control recording sector, and the second decipher key conversion data, which is a part of non-encrypted content in the sector for recording the encrypted content therein, another content decipher key is calculated which may be used as a content decipher key in the encrypting device 2120.

**[0184]** On the other hand, the key encrypting device 2118 encrypts the above inputted cipher key using a disk key inputted in the same way as that of the optical disk reproducing apparatus, and generates the encrypted decipher key. As compared with the size of this encrypted decipher key, each of the decipher key areas 2106 and 2109 in the sector header area is small, therefore, the data divider 2121 divides the encrypted decipher key into a plurality of divided decipher keys, and then, records the respective divided decipher keys into different decipher key areas 2106 and 2109. In an example of Fig. 37, the encrypted decipher key is divided into two encrypted divided decipher keys, which are then recorded in the decipher key areas 2106 and 2109 of two continuos sectors. In this case, since the decipher key of a cipher key is encrypted by the key encrypting device 2118, the security intensity of the encryption for the cipher key can be enhanced.

**[0185]** When the content is reproduced, the key converter 2113 performs an operation or calculation of a predetermined key conversion on the decipher key from the key decrypting device 2112, using information of the above-mentioned first decipher key conversion data 2115 and the second decipher key conversion data 2116 to generate the content decipher key, which is then outputted to the decrypting device 2114. Also, the decrypt-

ing device 2114 decrypts the data of the encrypted content using this content decipher key to obtain the decrypted content. In this case, the key converter 2113 may perform an operation or calculation of a predetermined key conversion on the decipher key from the key decrypting device 2112 using only the information of the first decipher key conversion data 2115.

## ELEVENTH PREFERRED EMBODIMENT

**[0186]** Fig. 38 is a block diagram showing a configuration of a user data area on an optical disk, a configuration of an optical disk recording apparatus for encrypting content and recording encrypted content in the user data area, and a configuration of an optical disk reproducing apparatus for decrypting an encrypted content from the data of the user data area, according to an eleventh preferred embodiment of the present invention. This eleventh preferred embodiment is characterized in that the configuration of the optical disk recording apparatus is added to that of the seventh preferred embodiment, and the configuration thereof will be described in detail.

**[0187]** Referring to Fig. 38, the optical disk recording apparatus comprises a key encrypting device 2118 for encrypting a cipher key using a predetermined disk key in the same way as that of the tenth preferred embodiment shown in Fig. 37, a key converter 2119 for operating or calculating a content decipher key through an operation of a predetermined key conversion on the cipher key by using the first and the second decipher key conversion data 2115 and 2116 in the content, and an encrypting device 2120 for encrypting the content using the above-mentioned content decipher key. In this case, the decipher key outputted from the key encrypting device 2118 is recorded in the main data area 2102 within the lead-in area 2401. On the other hand, the optical disk reproducing apparatus comprises a key decrypting device 2112, a key converter 2113, and a decrypting device 2114 in the same way as that of the seventh preferred embodiment shown in Fig. 29. In this case, the decipher key recorded in the main data area 2102 within the lead-in area 2401 is read out and is inputted to the key decrypting device 2112, which then decrypts the decipher key using a predetermined disk key and outputs the decrypted decipher key to the key converter 2113. Also, the key converter 2113 performs an operation or calculation of a predetermined key conversion on the decipher key from the key decrypting device 2112 by using the first and the second decipher key conversion data 2115 and 2116 to calculate the content decipher key, which is outputted to the decrypting device 2114.

## ADVANTAGEOUS EFFECTS OF SIXTH TO NINTH PREFERRED EMBODIMENTS

**[0188]** As described above, an optical disk of recording type according to the present preferred embodiments divides and records the decipher key into decipher keys of the decipher key areas having a predetermined size arranged in the sector header area, or records the decipher key having a variable length in the decipher key area indicated by the key index area arranged in the sector header area, and then, an optical disk of recording type which can utilize a decipher key of an arbitrary or free length regardless of a decipher key area of a size prescribed in the sector header area can be provided. Therefore, in accordance with the copyright protection level for the recorded content, it becomes possible to utilize the encryption using an arbitrary key length.

## MODIFIED PREFERRED EMBODIMENTS

**[0189]** In the above-mentioned preferred embodiments, the above-mentioned disk identification information is preferably constituted by pre-pits which are non-rewritable, and the above-mentioned disk identification information has preferably a region identifier for representing a region in which the optical disk is used. Also, the above-mentioned disk identification information has preferably a data category identifier representing a type, class or kind of content which is recordable and reproducible on the optical disk. In addition, the above-mentioned disk identification information is, preferably, encrypted using a secret key, and recorded in the disk identification information area upon manufacturing. Furthermore, the above-mentioned disk identification information preferably includes data for representing a type, class or kind of data which is recordable in the data recording and reproducing areas, or a type, class or kind of data which is reproducible from the data recording and reproducing area.

**[0190]** In the above-mentioned preferred embodiments, the above-mentioned optical disk preferably have a sector area for data of content therein, and a descramble area management table for managing the corresponding relationship with the descramble key. The key management information area preferably includes a descramble key area for recording a descramble key encrypted using disk identification information as a key, a key information area having a descramble key status area for representing a recording status or state of the descramble key, a content information area for recording therein key information used upon reproduction of the content recorded on the disk, and a key index area for recording therein a pointer for referring to a descramble key required for reproduction of the content. In addition, in the sector recording the data of the content, there are recorded preferably the data of the above content, and a pointer for indicating an area for recording the descramble key therein.

**[0191]** In the above-mentioned preferred embodiments, a reproducing circuit of the disk identification information of the optical disk recording and reproducing apparatus preferably comprises a circuit for decrypting

disk identification information which has been encrypted using a secret key. Also, in the optical disk recording and reproducing apparatus, the data encrypted with the disk identification information as a key are preferably data of content such as image data and music data. In addition, the disk identification information preferably represents a type, class or kind of data which is recordable in the data recording and reproducing area, and the reproducing circuit of the disk identification information determines whether or not the data is of recordable content by the type, class or kind of the above-mentioned data. Furthermore, the data which is decrypted using the disk identification information as a key is preferably data of the content such as image data or music data. Also, the disk identification information preferably represents a type, class or kind of data which is reproducible from the data recording and reproducing area, and the reproducing circuit determines whether or not the data is of reproducible content based on the type, class or kind of the above-mentioned data.

**[0192]** In the above-mentioned preferred embodiments, the recording circuit of the content preferably records data of content such as encrypted image data and music data and the descramble key for decoding or decrypting encryption of the data of the above-mentioned content, in the same sector. Also, the reproducing circuit of the content preferably reproduces data of content such as encrypted image data and music data and the descramble key for decoding or decrypting encryption of the data of the above-mentioned content from the same sector.

**[0193]** In the above-mentioned preferred embodiment, a circuit or a method for allocating key areas preferably arranges a flag for reserved area in a descramble key status area for representing a recorded status of the descramble key, records information with respect to a key used upon reproduction of the data of the content, and records a key index for representing a recording area of the descramble key allocated for the data of the content. Also, a circuit or a method for arranging the descramble key preferably reproduces an index of a descramble key area used in the content from the content information area, arrange a descramble key into a descramble key area indicated in a key index corresponding to the recorded descramble key, and arrange a flag of recorded information in a descramble key status area indicated in the key index corresponding to the recorded descramble key.

**[0194]** In the above preferred embodiment, the optical disk reproducing apparatus preferably reproduces disk identification information, searches whether or not content is reproducible, reproduces key management information, reproduces a sector in which data of content such as image data or music data have been recorded, and acquires a descramble key from the reproduced sector. In addition, preferably, the data of the reproduced content is descrambled by the descramble key, and the descrambled data is outputted.

**[0195]** In the above-mentioned preferred embodiments, the method for recording data of content preferably records encrypted content so as to be able to be decoded and reproduced through an operation or calculation using at least the above-mentioned second disk information, when the content is recorded in the user data area of an optical disk having a first information area for recording first disk information therein, a second information area for recording therein second disk information for identifying individual disks and the user data area for recording information by irradiating a light beam onto the user data area.

**[0196]** In the above-mentioned preferred embodiments, the method for recording data of content is preferably to encrypt and record information so as to be decoded and reproduced by an operation or calculation using at least the second disk information and the key information, when recording the content in the above-mentioned user data area of the optical disk having a first information area for recording first disk information therein, a second information area for recording therein second disk information for identifying individual disks, a user data area for recording information by irradiating a light beam onto the user data area, and a key information recording area for recording key information for decode or decrypting content encrypted and recorded within the user data area.

**[0197]** In the above-mentioned preferred embodiments, dummy data is recorded in a sector of an optical disk having a decipher key area for recording a plurality of divided decipher keys in a plurality of continuous sectors, preferably in the main data area in which a data size including the AV data is less than (main data size) × (number of divided decipher keys). Also, in the ECC block, the sector having a decipher key area for recording divided decipher keys divided into a plurality of continuous sectors is recorded (ECC block unit)/(number of divided decipher keys) times, and the dummy data is recorded in the main data area in which data size including AV data is less than (main data size) × (ECC block unit).

**[0198]** In the above-mentioned preferred embodiments, a decipher key for decrypting encryption which has been performed on data including the AV data is preferably divided into a plurality of divided decipher keys with a predetermined size, and the plurality of divided decipher keys are recorded in a plurality of decipher key areas in which decipher key table continues. Also, the above-mentioned decipher key table is preferably recorded in the main data area within the rewritable lead-in area. In addition, information for representing a the recording status or state of the decipher key table is preferably recorded in each decipher key area of the decipher key table as a fixed value. Furthermore, the decipher key table is recorded a plurality of times in the above-mentioned different ECC blocks arranged in the inner and the outer peripheries of the optical disk.

**[0199]** In the above-mentioned preferred embodi-

ments, the encoding apparatus 3101 of a data encrypting apparatus, and the optical disk apparatus 3102 of an optical disk recording and reproducing apparatus, preferably share the bus key in a mutual authorization system. Also, the decoding apparatus 3103 of a data decoding apparatus, and an optical disk apparatus 3102 of an optical disk recording and reproducing apparatus, preferably, share the bus key in a cross authenticating system.

**[0200]** Although, in the above-mentioned preferred embodiment, an optical disk of recording type which can record data, and which is either write-once type or rewritable type including a RAM type or non-rewritable optical disk, is described, the present invention is not limited to this. The present invention can be applied for read-only type optical disk which can read out and reproduce the previously recorded data but can not newly record data. In the case of a read-only type optical disk, the data recording and reproducing area can be replaced with the data reproducing area which reads out and reproduces the data, and the data of the content or the data of other various control information is previously recorded upon manufacturing. In this case, the optical disk of recording type includes CD-R, CD-RW, MO, MD, DVD-RAM and so forth. The read-only type optical disk includes music CD, CD-ROM, DVD-ROM and so forth.

ADVANTAGEOUS EFFECTS OF THE INVENTION

**[0201]** As described above in detail, according to an optical disk of the present invention, disk identification information using which recording operation and reproducing operation are performed for each optical disk is recorded in a produce-only area which is non-rewritable, the recording operation and the reproduction operation of the content onto or from the optical disk can be controlled by the user, utilizing the information recorded upon manufacture of the optical disk.

**[0202]** Also, according to an optical disk of the present invention, data, which has been encrypted using the read-only disk identification information which is impossible to be rewritten, as a key, is recorded in the user data area of the optical disk, and therefore, even in the case that the user data area is copied onto another optical disk of recording type by the user, the disk identification information can not be copied so that correct decryption and reproduction of the data becomes impossible.

**[0203]** In addition, according to an optical disk of the present invention, encrypted data and a descramble key for decrypting encryption are recorded in sector areas different from each other, and it becomes possible to acquire data such as movies and music required for copyright protection and to acquire a descramble key for descrambling encryption independently. Moreover, by encrypting and recording the descramble key using the disk identification information as a key, the disk identification information can not be copied, which makes it impossible to correctly record and reproduce the data even if the user data area is copied onto another optical disk of recording type by the user. By acquiring and recording the descramble key which has been encrypted using the disk identification information of the optical disk onto which the data are copied as a key, this makes it possible to correctly record and reproduce the data.

**[0204]** Moreover, an optical disk according to the present invention comprises a first information area for recording a first disk information therein, a second information area for recording a second disk information for identifying individual disks, and a user data area for recording information by irradiating a light beam onto the user data area. Accordingly, by adding information for identifying the above-mentioned optical disk to an optical disk according to the prior art, the management of optical disks can easily be implemented. In this case, the above-mentioned second information area is preferably recorded in the above-mentioned first information area, and data of the second information area can be reproduced by an optical pick up for reproducing the above-mentioned first information area. Also, the above-mentioned second information area is recorded by partially eliminating or removing a recording film within the above-mentioned first information area, so that a plurality of trimming areas having an elongated shape in the radius direction are formed, and this leads to that easy falsification of the above-mentioned second disk information can be prevented.

**[0205]** In addition, according to an optical disk of the present invention, a decipher key is divided into a plurality of divided decipher keys which are then allocated in decipher key areas each having a predetermined size arranged in the sector header area, or a decipher key is recorded in the decipher key areas indicated by an key index area arranged in the sector header area. This leads to that an optical disk of recording type can be provided which can utilize the decipher key having an arbitrary or free length, independently of the decipher key area having a prescribed size in the sector header area. Therefore, it becomes possible to use an encryption using an arbitrary key length in accordance with the level of copyright protection level for recorded content.

**[0206]** Although the present invention has been fully described in connection with the preferred embodiments thereof with reference to the accompanying drawings, it is to be noted that various changes and modifications are apparent to those skilled in the art. Such changes and modifications are to be understood as included within the scope of the present invention as defined by the appended claims unless they depart therefrom.

## Claims

1. An optical disk (100) of recording type on which data is recordable,

wherein said optical disk (100) has a sector structure comprising a plurality of sectors, wherein each of the sectors (401) includes a sector header area (402) and a main data area (403) for recording encrypted content data therein,
**characterized in that** the sector header area (402) includes a descramble key information area (408) for recording therein a key index for indicating a recorded position of a descramble key required for decrypting the encrypted data within a descramble key table (505) of a key management information area (107),
wherein a size of the descramble key information area (408) is smaller than that of each descramble key, and
wherein said respective descramble keys are recorded in said descramble key table (505) having a plurality of descramble keys.

2. The optical disk as claimed in claim 1,
wherein descramble key status areas (506) for recording descramble key statuses on the respective descramble keys of the descramble key table (505) are recorded as information for representing a recorded status of the descramble key table (505).

3. The optical disk as claimed in claim 1,
wherein the descramble key table (505) is recorded over a plurality of different error correction code (ECC) blocks.

4. The optical disk as claimed in claim 1,
wherein the respective descramble keys are managed and recorded in at least one unit of a file unit managed in a file management area, and an extent unit comprising a plurality of continuous sectors on the optical disk.

5. An optical disk recording apparatus comprising:

first recording means (703) for recording encrypted content data in a main data area (403) of an optical disk, said optical disk (100) having a sector structure comprising a plurality of sectors, wherein each of the sectors (401) includes a sector header area (402) and a main data area (403),
first acquiring means (5803) for acquiring the descramble key required for reproducing the encrypted data.
second recording means (703) for recording in a descramble key information area (408) of the sector header area (402) a key index for indicating a recorded position of a descramble key required for decrypting the encrypted data within a descramble key table (505) wherein a size of the descramble key information area (408) is smaller than that of each descramble key, and
third recording means (703) for recording the respective descramble keys in said descramble key table (505) of a key management information area (107) having a plurality of descramble keys.

6. The optical disk recording apparatus as claimed in claim 5, further comprising:

second acquiring means (S901) for acquiring a descramble key required for recording content data; and
allocating means (S902, S905) for reproducing the descramble key recorded in the key management information area (107), and allocating an area for recording the reproduced descramble key and the acquired descramble key in the key management information area (107).

7. The optical disk recording apparatus as claimed in claim 6, further comprising:

third acquiring means (S1003) for acquiring a descramble key required for reproducing content data; and
third recording means (S1007) for reproducing a descramble key recorded in the key management information area (107), and recording the acquired descramble key in the key management information area (107) based on the reproduced descramble key.

8. The optical disk recording apparatus as claimed in claim 7,
wherein said optical disk (701, 100) includes a disk identification information area (106) for recording therein a disk identification information for identifying said optical disk,
wherein said optical disk recording apparatus further comprises:

reproducing means (S801) for reproducing the disk identification information from the disk identification information area (106); and
judging means (S802) for judging whether or not content data is to be recorded in said optical disk based on the reproduced disk identification information.

9. An optical disk recording method comprising the steps of:

recording encrypted content data in a main data area (403) of an optical disk, said optical disk (100) having a sector structure comprising a plurality of sectors, wherein each of the sectors (401) includes a sector header area (402) and a main data area (403),

acquiring the descramble key required for reproducing the encrypted data,
recording in a descramble key information area (408) of the sector header area (402) a key index for indicating a recorded position of a descramble key required for decrypting the encrypted data within a descramble key table (505) wherein a size of the descramble key information area (408) is smaller than that of each descramble key, and
recording the respective descramble keys in said descramble key table (505) of a key management information area (107) having a plurality of descramble keys.

**10.** The optical disk recording method as claimed in claim 9, further including the steps of:

acquiring (S901) a descramble key required for recording content data; and
reproducing (S902, S905) the descramble key recorded in the key management information area (107); and allocating an area for recording the reproduced descramble key and the acquired descramble key in the key management information area (107).

**11.** The optical disk recording method as claimed in claim 9, further including the steps of:

acquiring (S1003) a descramble key required for reproducing content data; and
reproducing (S1007) a descramble key recorded in the key management information area (107), and recording the acquired descramble key in the key management information area (107) based on the reproduced descramble key.

**12.** The optical disk recording method as claimed in claim 9,
wherein said optical disk (701, 100) includes a disk identification information area (106) for recording therein a disk identification information for identifying said optical disk,
wherein said optical disk recording method further includes the step of:

reproducing (S801) the disk identification information from the disk identification information area (106); and
judging (S802) whether or not content data is to be recorded in said optical disk based on the reproduced disk identification information.

**13.** An optical disk reproducing apparatus for reproducing data recorded on an optical disk of recording type on which data is recordable, wherein said optical disk (701, 100) has a sector structure comprising a plurality of sectors, wherein each of the sectors (401) includes a sector header area (402) and a main data area (403), comprising:

first reproducing means (S1903) for reproducing content data from a main data area of a sector;
judging means (S1201) for judging, based on the reproduced content data, whether or not the content data is scrambled;
second reproducing means (S1202) for reproducing a key index from a descramble key information area (408) of the sector header area (402) of the same sector from which content data have been reproduced by said first reproducing means when judging that said content data is scrambled,
third reproducing means (S1203) for acquiring and reproducing a descramble key from a descramble key table (505) of a key management information area (107) based on the reproduced key index, and
fourth reproducing means (S1109) for decrypting the encrypted content data using said descramble key.

**14.** The optical disk reproducing apparatus as claimed in claim 13,
further comprising a reproducing means (S1101) for reproducing a disk identification information from a disk identification information area and
a decrypting means (S1206) for reproducing the descramble key by decrypting the encrypted descramble key by decrypting the encrypted descramble key using the reproduced disk identification information as a key.

**15.** The optical disk reproducing apparatus as claimed in claim 14,
wherein an error detection code is given to the decrypted descramble key, and
wherein said decrypting means (S1204) judges whether or not there is an error in the decrypted descramble key, based on the error detection code which is given to the decrypted descramble key, and judges whether or not the decrypted descramble key should be reproduced based on a judgement result.

**16.** An optical disk reproducing method for reproducing data recorded on an optical disk of recording type on which data is recordable, wherein said optical disk (701, 100) has a sector structure comprising a plurality of sectors, wherein each of the sectors (401) includes a sector header area (402) and a main data area (403), comprising the steps of:

reproducing content data from a main data area of a sector;
judging, based on the reproduced content data, whether or not the content data is scrambled;
reproducing a key index from a descramble key information area (408) of the sector header area (402) of the same sector from which content data have been reproduced by said first reproducing means when judging that said content data is scrambled,
acquiring and reproducing a descramble key from a descramble key table (505) of a key management information area (107) based on the reproduced key index, and
decrypting the encrypted content data using said descramble key.

**Patentansprüche**

1. Optische Disk (100) des Aufzeichnungstyps, auf welcher Daten aufgezeichnet werden können, wobei die optische Disk (100) eine Sektorstruktur aufweist, mit einer Mehrzahl von Sektoren, bei welcher jeder der Sektoren (401) einen Sektor-Kopfbereich (402) und einen Hauptdatenbereich (403) zum Aufzeichnen verschlüsselter Inhaltsdaten darin aufweist,
**dadurch gekennzeichnet, dass** der Sektor-Kopfbereich (402) einen Entschlüsselungs-Schlüssel-Informationsbereich (408) beinhaltet, zum Aufzeichnen eines Schlüssel-Index darin zum Angeben einer Aufzeichnungsposition eines Entschlüsselungs-Schlüssels, welcher erforderlich ist zum Entschlüsseln der verschlüsselten Daten, innerhalb einer Entschlüsselungs-Schlüssel-Tabelle (505) eines Schlüssel-Verwaltungsinformationsbereiches (107),
wobei eine Größe des Entschlüsselungs-Schlüssel-Informationsbereiches (408) geringer ist diejenige jedes Entschlüsselungs-Schlüssels, und
wobei die entsprechenden Entschlüsselungs-Schlüssel in der Entschlüsselungs-Schlüssel-Tabelle (505) mit einer Mehrzahl von Entschlüsselungs-Schlüsseln aufgezeichnet sind.

2. Optische Disk nach Anspruch 1,
bei welcher Entschlüsselungs-Schlüssel-Statusbereiche (506) zum Aufzeichnen von Entschlüsselungs-Schlüssel-Stati der entsprechenden Entschlüsselungs-Schlüssel der Entschlüsselungs-Schlüssel-Tabelle (505) als Information aufgezeichnet werden zum Darstellen eines aufgezeichneten Status der Entschlüsselungs-Schlüssel-Tabelle (505).

3. Optische Disk nach Anspruch 1,
bei welcher die Entschlüsselungs-Schlüssel-Tabelle (505) über eine Mehrzahl verschiedener Fehlerkorrekturkode(ECC)-Blbcke aufgezeichnet ist.

4. Optische Disk nach Anspruch 1,
bei welcher die entsprechenden Entschlüsselungs-Schlüssel in wenigstens einer Einheit einer Dateieinheit verwaltet und aufgezeichnet werden, die in einem Datei-Verwaltungsbereich verwaltet wird, und eine Erweiterungseinheit mit einer Mehrzahl fortlaufender Sektoren auf der optischen Disk.

5. Aufzeichnungsvorrichtung für eine optische Disk, mit:

einer ersten Aufzeichnungseinrichtung (703) zum Aufzeichnen verschlüsselter Inhaltsdaten in einem Hauptdatenbereich (403) einer optischen Disk, wobei die optische Disk (100) eine Sektorstruktur mit einer Mehrzahl von Sektoren aufweist, wobei jeder der Sektoren (401) einen Sektor-Kopfbereich (402) und einen Hauptdatenbereich (403) enthält,
einer ersten Erhalte-Einrichtung (5803) zum Erhalten des zum Wiedergeben der verschlüsselten Daten benötigten Entschlüsselungs-Schlüssels,
einer zweiten Aufzeichnungseinrichtung (703) zum Aufzeichnen eines Schlüssel-Index in einem Entschlüsselungs-Schlüssel-Informationsbereich (408) des Sektor-Kopfbereiches (402) zum Anzeigen einer aufgezeichneten Position eines zum Entschlüsseln der verschlüsselten Daten erforderlichen Entschlüsselungs-Schlüssels in einer Entschlüsselungs-Schlüssel-Tabelle (505), wobei eine Größe des Entschlüsselungs-Schlüssel-Informationsbereichs (408) geringer ist als diejenige jedes Entschlüsselungs-Schlüssels, und
einer dritten Aufzeichnungseinrichtung (703) zum Aufzeichnen der entsprechenden Entschlüsselungs-Schlüssel in der Entschlüsselungs-Schlüssel-Tabelle (505) eines Schlüssel-Verwaltungs-Informationsbereichs (107) mit einer Mehrzahl von Entschlüsselungs-Schlüsseln.

6. Aufzeichnungsvorrichtung für eine optische Disk nach Anspruch 5, und mit:

einer zweiten Erhalte-Einrichtung (S901) zum Erhalten eines zum Aufzeichnen von Inhaltsdaten erforderlichen Entschlüsselungs-Schlüssels; und
einer Zuordnungseinrichtung (S902, S905) zum Wiedergeben des in dem Schlüssel-Verwaltungsinformationsbereich (107) aufgezeichneten Entschlüsselungs-Schlüssels, und zum Zuordnen eines Bereiches zum Aufzeich-

nen des wiedergegebenen Entschlüsselungs-Schlüssels und des erworbenen Entschlüsselungs-Schlüssels in dem Schlüssel-Verwaltungsinformationsbereich (107).

7. Aufzeichnungsvorrichtung für eine optische Disk nach Anspruch 6, und mit:

einer dritten Erhalte-Einrichtung (S1003) zum Erhalten eines zum Wiedergeben von Inhaltsdaten erforderlichen Entschlüsselungs-Schlüssels; und
einer dritten Aufzeichnungseinrichtung (S1007) zum Wiedergeben eines in dem Schlüssel-Verwaltungsinformationsbereich (107) aufgezeichneten Entschlüsselungs-Schlüssels und Aufzeichnen des erhaltenen Entschlüsselungs-Schlüssels in dem Schlüssel-Verwaltungsinformationsbereich (107) basierend auf dem wiedergegebenen Entschlüsselungs-Schlüssel.

8. Aufzeichnungsvorrichtung für eine optische Disk nach Anspruch 7,
bei welcher die optische Disk (701, 100) einen Diskidentifizierungs-Informationsbereich (106) beinhaltet, zum Aufzeichnen einer Diskidentifizierungsinformation darin zum identifizieren der optischen Disk,
wobei die Aufzeichnungsvorrichtung für eine optische Disk weiterhin umfasst:

eine Wiedergabeeinrichtung (S801) zum Wiedergeben der Diskidentifizierungsinformation von dem Diskidentifizierungs-Informationsbereich (106); und
eine Beurteilungseinrichtung (S802) zum Beurteilen, ob Inhaltsdaten auf der optischen Disk aufzuzeichnen sind oder nicht, basierend auf der wiedergegebenen Diskidentifizierungsinformation.

9. Aufzeichnungsverfahren für eine optische Disk, mit den Schritten:

Aufzeichnen verschlüsselter Inhaltsdaten in einem Hauptdatenbereich (403) einer optischen Disk, wobei die optische Disk (100) eine Sektorstruktur mit einer Mehrzahl von Sektoren aufweist, wobei jeder der Sektoren (401) einen Sektor-Kopfbereich (402) und einen Hauptdatenbereich (403) aufweist,
Erhalten des zum Wiedergeben der verschlüsselten Daten erforderlichen Entschlüssefungs-Schlüssels,
Aufzeichnen eines Schlüssel-Index in einem Entschlüsselungs-Schlüssel-Informationsbereich (408) des Sektor-Kopfbereiches (402) zum Angeben einer aufgezeichneten Position eines zum Entschlüsseln verschlüsselter Daten erforderlichen Entschlüsselungs-Schlüssels innerhalb einer Entschlüsselungs-Schlüssel-Tabelle, wobei eine Größe des Entschlüsselungs-Schlüssel-Informationsbereichs (408) geringer ist, als diejenige jedes Entschlüsselungs-Schlüssels; und
Aufzeichnen der entsprechenden Entschlüsselungs-Schlüssel in der Entschlüsselungs-Schlüssel-Tabelle (505) eines Schlüssel-Verwaltungsinformationsbereichs (107) mit einer Mehrzahl von Entschlüsselungs-Schlüsseln.

10. Aufzeichnungsverfahren für eine optische Disk nach Anspruch 9, und mit den Schritten:

Erhalten (S901) eines zum Aufzeichnen von Inhaltsdaten erforderlichen Entschlüsselungs-Schlüssels; und
Wiedergeben (S902, S905) des in dem Schlüssel-Verwaltungsinformationsbereich (107) aufgezeichneten Entschlüsselungs-Schlüssels, und Zuordnen eines Bereichs zum Aufzeichnen des wiedergegebenen Entschlüsselungs-Schlüssels und des erhaltenen Entschlüsselungs-Schlüssels in dem Schlüssel-Verwaltungsinformationsbereich (107).

11. Aufzeichnungsverfahren für eine optische Disk nach Anspruch 9, und mit den Schritten:

Erhalten (S1003) eines zum Wiedergeben von Inhaltsdaten erforderlichen Entschlüsselungs-Schlüssels; und
Wiedergeben (S1007) eines in dem Schlüssel-Verwaltungsinformationsbereich (107) aufgezeichneten Entschlüsselungs-Schlüssels und Aufzeichnen des erhaltenen Schlüssels in dem Schlüssel-Verwaltungsinformationsbereich (107) basierend auf dem wiedergegebenen Entschlüsselungs-Schlüssel.

12. Aufzeichnungsverfahren für eine optische Disk nach Anspruch 9,
bei welchem die optische Disk (701, 100) einen Diskidentifizierungsinformationsbereich (106) enthält, um darin eine Diskidentifizierungsinformation zum Identifizieren der optischen Disk aufzuzeichnen,
wobei das Aufzeichnungsverfahren für eine optische Disk weiterhin den Schritt beinhaltet:

Wiedergeben (S801) der Diskidentifizierungsinformation aus dem Diskidentifizierungs-Informationsbereich (106); und
Beurteilen (S802), ob Inhaltsdaten auf der optischen Disk aufzuzeichnen sind oder nicht, basierend auf der wiedergegebenen Diskidentifi-

zierungsinformation.

13. Wiedergabevorrichtung für eine optische Disk zum Wiedergeben von aufgezeichneten Daten auf einer optischen Disk vom Aufzeichnungstyp, auf welcher Daten aufgezeichnet werden können, wobei die optische Disk (701, 100) eine Sektorstruktur aufweist, mit einer Mehrzahl von Sektoren,
wobei jeder der Sektoren (401) einen Sektor-Kopfbereich (402) und einen Hauptdatenbereich (403) umfasst, mit:

einer ersten Wiedergabeeinrichtung (S1103) zum Wiedergeben von Inhaltsdaten aus einem Hauptdatenbereich eines Sektors;
einer Beurteilungseinrichtung (S1201) zum Beurteilen, basierend auf den wiedergegebenen Inhaltsdaten, ob die Inhaltsdaten verschlüsselt sind oder nicht;
einer zweiten Wiedergabeeinrichtung (S1202) zum Wiedergeben eines Schlüssel-Index aus einem Entschlüsselungs-Schiüssel-Infarmationsbereich (408) des Sektor-Kopfbereiches (402) des gleichen Sektors, aus dem die Inhaltsdaten von der ersten Wiedergabeeinrichtung beim Beurteilen, ob die Inhaltsdaten verschlüsselt sind, wiedergegeben wurden,
einer dritten Wiedergabeeinrichtung (S1203) zum Erhalten und Wiedergeben eines Entschlüsselungs-Schlüssels aus einer Entschlüsselungs-Schlüssel-Tabelle (505) eines Schlüssel-Verwaltungsinformationsbereichs (107) basierend auf dem wiedergegebenen Schlüssel-Index; und
einer vierten Wiedergabeeinrichtung (S1109) zum Entschlüsseln der verschlüsselten Inhaltsdaten unter Verwendung des Entschlüsselungs-Schlüssels.

14. Wiedergabevorrichtung für eine optische Disk nach Anspruch 13,
und mit einer Wiedergabeeinrichtung (S1101) zum Wiedergeben einer Diskidentifizierungsinformation aus einem Diskidentifizierungs-Informationsbereich und
einer Entschlüsselungseinrichtung (S1206) zum Wiedergeben des Entschlüsselungs-Schlüssels durch Entschlüsseln des verschlüsselten Entschlüsselungs-Schlüssels durch Entschlüsseln des verschlüsselten Entschlüsselungs-Schlüssels unter Verwendung der wiedergegebenen Diskidentifizierungsinformation als ein Schlüssel.

15. Wiedergabevorrichtung für eine optische Disk nach Anspruch 14,
bei welcher dem verschlüsselten Entschlüsselungs-Schlüssel ein Fehlererfassungskode gegeben wird, und bei welcher die Entschlüsselungseinrichtung (S1204) beurteilt, ob ein Fehler in dem verschlüsselten Entschlüsselungs-Schlüssel ist oder nicht, basierend auf dem Fehlererfassungskode, welcher dem verschlüsselten Entschlüsselungs-Schlüssel gegeben wird, und basierend auf dem Beurteilungsergebnis beurteilt, ob der verschlüsselte Entschlüsselungs-Schlüssel wiedergegeben werden soll oder nicht.

16. Wiedergabeverfahren für eine optische Disk zum Wiedergeben von auf einer optischen Disk des Aufzeichnungstyps aufgezeichneten Daten, auf welcher Daten aufgezeichnet werden können, wobei die optische Disk (701, 100) eine Sektorstruktur mit einer Mehrzahl von Sektoren aufweist,
wobei jeder der Sektoren (401) einen Sektor-Kopfbereich (402) und einen Hauptdatenbereich (403) beinhaltet, mit den Schritten:

Wiedergeben von Inhaltsdaten aus einem Hauptdatenbereich eines Sektors;
Beurteilen, basierend auf den wiedergegebenen Inhaltsdaten, ob die Inhaltsdaten verschlüsselt sind oder nicht;
Wiedergeben eines Schlüssel-Index aus einem Entschlüsselungs-Schlüssel-Informationsbereich (408) des Sektor-Kopfbereichs (402) des gleichen Sektors, aus welchem Inhaltsdaten von der ersten Wiedergabeeinrichtung wiedergegeben wurden, wenn beurteilt wurde, dass die Inhaltsdaten verschlüsselt sind,
Erhalten und Wiedergeben eines Entschlüsselungs-Schlüssels aus einer Entschlüsselungs-Schlüssel-Tabelle (505) eines Schlüssel-Verwaltungsinformationsbereichs (107) basierend auf dem wiedergegebenen Schlüssel-Index, und
Entschlüsseln der verschlüsselten Inhaltsdaten unter Verwendung des Entschlüsselungs-Schlüssels.

**Revendications**

1. Disque optique (100) de type enregistrement, sur lequel des données sont enregistrables,
dans lequel ledit disque optique (100) possède une structure par secteurs comprenant une pluralité de secteurs, dans lesquels chacun des secteurs (401) comprend une zone d'en-tête de secteur (402) et une zone principale de données (403) destinée à l'enregistrement de données de contenu cryptées dans celle-ci,
**caractérisé en ce que** la zone d'en-tête de secteur (402) comprend une zone (408) d'informations de clés de décryptage destinée à y enregistrer un index de clé destiné à indiquer une position enregistrée d'une clé de décryptage nécessaire au dé-

cryptage des données cryptées dans un tableau (505) de clés de décryptage d'une zone (107) d'informations de gestion de clés,

dans lequel une taille de la zone (408) d'information de clés de décryptage est plus petite que celle de chaque clé de décryptage, et

dans lequel lesdites clés de décryptage sont enregistrées dans ledit tableau (505) de clés de décryptage comportant une pluralité de clés de décryptage.

2. Disque optique selon la revendication 1,

dans lequel les zones (506) d'état des clés de décryptage destinées à enregistrer les états des clés de décryptage sur les clés de décryptage respectives du tableau (505) des clés de décryptage sont enregistrées en tant qu'information destinée à représenter un état enregistrer du tableau (505) de clés de décryptage.

3. Disque optique selon la revendication 1,

dans lequel le tableau (505) de clés de décryptage est enregistré sur une pluralité de blocs différents de code de correction d'erreur (ECC).

4. Disque optique selon la revendication 1,

dans lequel les clés de décryptage respectives sont gérées et enregistrées dans au moins une unité d'une unité de fichier gérée dans une zone de gestion de fichiers, et une unité d'extension comprenant une pluralité de secteurs continus sur le disque optique.

5. Appareil d'enregistrement sur disque optique comprenant :

un premier moyen d'enregistrement (703) destiné à enregistrer des données de contenu cryptées dans une zone principale de données (403) d'un disque optique, ledit disque optique (100) possédant une structure par secteurs comprenant une pluralité de secteurs, dans lesquels chacun des secteurs (401) comprend une zone d'en-tête de secteur (402) et une zone principale de données (403),

un premier moyen d'acquisition (S803) destiné à acquérir la clé de décryptage nécessaire à la reproduction des données cryptées,

un deuxième moyen d'enregistrement (703) destiné à enregistrer dans une zone (408) d'informations de clés de décryptage de la zone (402) d'en-tête de secteur des index de clé destinés à indiquer une position enregistrée d'une clé de décryptage nécessaire au décryptage des données cryptées dans un tableau (505) de clés de décryptage, dans lequel une taille de la zone (408) d'informations de clés de décryptage est plus petite que celle de chaque clé de décryptage, et

un troisième moyen d'enregistrement (703) destiné à enregistrer les clés de décryptage respectives dans ledit tableau (505) de clés de décryptage d'une zone (107) d'informations de gestion de clés comprenant une pluralité de clés de décryptage.

6. Appareil d'enregistrement sur disque optique selon la revendication 5, comprenant en outre :

un deuxième moyen d'acquisition (S901) destiné à acquérir une clé de décryptage nécessaire à l'enregistrement de données de contenu ; et

des moyens d'affectation (S902, S905) destinés à reproduire la clé de décryptage enregistrée dans la zone (107) d'informations de gestion de clés, et à affecter une zone destinée à l'enregistrement de la clé de décryptage reproduite et de la clé de décryptage acquise dans la zone (107) d'informations de gestion de clés.

7. Appareil d'enregistrement sur disque optique selon la revendication 6, comprenant en outre :

un troisième moyen d'acquisition (S1003) destiné à acquérir une clé de décryptage nécessaire à la reproduction des données de contenu ; et

un troisième moyen d'enregistrement (S1007) destiné à reproduire une clé de décryptage enregistrée dans la zone (107) d'informations de gestion de clés, et à enregistrer la clé de décryptage acquise dans la zone (107) d'informations de gestion de clés en se basant sur la clé de décryptage reproduite.

8. Appareil d'enregistrement sur disque optique selon la revendication 7,

dans lequel ledit disque optique (701, 100) comprend une zone (106) d'informations d'identification de disque destinée à y enregistrer une information d'identification de disque destinée à identifier ledit disque optique,

dans lequel ledit appareil d'enregistrement sur disque optique comprend en outre :

un moyen de reproduction (S801) destinée à reproduire l'information d'identification de disque à partir de la zone (106) d'informations d'identification de disque ; et

un moyen de jugement (S802) destiné à juger si les données de contenu doivent ou non être enregistrées dans ledit disque optique en se basant sur l'information d'identification de disque reproduite.

9. Procédé d'enregistrement sur disque optique comprenant les étapes consistant à :

enregistrer des données de contenu cryptées dans une zone principale de données (403) d'un disque optique, ledit disque optique (100) possédant une structure par secteurs comprenant une pluralité de secteurs, dans lesquels chacun des secteurs (401) comprend une zone d'entête de secteur (402) et une zone principale de données (403),
acquérir la clé de décryptage nécessaire à la reproduction des données cryptées,
enregistrer dans une zone (408) d'informations de clés de décryptage de la zone (402) d'entête de secteur un index de clé destiné à indiquer une position enregistrée d'une clé de décryptage nécessaire au décryptage des données cryptées dans un tableau (505) de clés de décryptage, dans lequel une taille de la zone (408) d'information de clés de décryptage est plus petite que celle de chaque clé de décryptage, et
enregistrer les clés de décryptage respectives dans ledit tableau (505) de clés de décryptage d'une zone (107) d'informations de gestion de clés comprenant une pluralité de clés de décryptage.

10. Procédé d'enregistrement sur disque optique selon la revendication 9, comprenant en outre les étapes consistant à :

acquérir (S901) une clé de décryptage nécessaire à l'enregistrement des données de contenu ; et reproduire (S902, S905) la clé de décryptage enregistrée dans la zone (107) d'informations de gestion de clés ; et affecter une zone destinée à enregistrer la clé de décryptage reproduite et la clé de décryptage acquise dans la zone (107) d'informations de gestion de clés.

11. Procédé d'enregistrement sur disque optique selon la revendication 9, comprenant en outre les étapes consistant à :

acquérir (S1003) une clé de décryptage nécessaire à la reproduction des données de contenu ; et reproduire (S1007) une clé de décryptage enregistrée dans la zone (107) d'informations de gestion de clés et enregistrer la clé de décryptage acquise dans la zone (107) d'informations de gestion de clés en se basant sur la clé de décryptage reproduite.

12. Procédé d'enregistrement sur disque optique selon la revendication 9,

dans lequel ledit disque optique (701, 100) comprend une zone (106) d'informations d'identification de disque destinée à y enregistrer une information d'identification de disque destinée à identifier ledit disque optique,

dans lequel ledit procédé d'enregistrement sur disque optique comprend en outre l'étape consistant à :

reproduire (S801) l'information d'identification de disque à partir de la zone (106) d'informations d'identification de disque ; et
juger (S802) si les données de contenu doivent ou non être enregistrées dans ledit disque optique en se basant sur l'information d'identification de disque reproduite.

13. Appareil d'enregistrement sur disque optique destiné à reproduire des données enregistrées sur un disque optique de type enregistrement sur lequel des données sont enregistrables, dans lequel ledit disque optique (701, 100) possède une structure par secteurs comprenant une pluralité de secteurs, dans lesquels chacun des secteurs (401) comprend une zone d'en-tête de secteur (402) et une zone principale de données (403), comprenant:

un premier moyen de reproduction (S1103) destiné à reproduire des données de contenu à partir d'une zone principale de données d'un secteur ;
un moyen de jugement (S1201) destiné à juger, en se basant sur les données de contenu reproduites, si les données de contenu sont ou non cryptées ;
un deuxième moyen de reproduction (S1202) destiné à reproduire un index de clé à partir d'une zone (408) d'informations de clés de décryptage de la zone (402) d'en-tête de secteur du même secteur à partir duquel les données de contenu ont été reproduites par ledit premier moyen de reproduction quand il est jugé que lesdites données de connues sont cryptées,
un troisième moyen de reproduction (S1203) destiné à acquérir et à reproduire une clé de décryptage à partir d'un tableau (505) de clés de décryptage d'une zone (107) d'informations de gestion de clés en se basant sur l'index de clé reproduit, et
un quatrième moyen de reproduction (S1109) destiné à décrypter les données de contenu cryptées au moyen de ladite clé de décryptage.

14. Appareil d'enregistrement sur disque optique selon la revendication 13, comprenant en outre un moyen de reproduction (S1101) destiné à reproduire une information d'identification de disque à partir d'une zone d'informations d'identification de disque et

un moyen de décryptage (S1206) destiné à reproduire la clé de décryptage par décryptage de la clé de décryptage cryptée au moyen de l'information d'identification de disque en tant que clé.

15. Appareil d'enregistrement sur disque optique selon la revendication 14,
dans lequel un code de détection d'erreur est donné à la clé de décryptage décryptée, et dans lequel ledit moyen de décryptage (S1204) juge s'il y a ou non une erreur dans la clé de décryptage décryptée, en se basant sur le code de détection d'erreur qui est donné à la clé de décryptage décryptée, et juge si la clé de décryptage décryptée doit ou non être reproduite en se basant sur un résultat de jugement.

16. Procédé de reproduction sur disque optique destiné à reproduire des données enregistrées sur un disque optique de type enregistrement, sur lequel des données sont enregistrables, dans lequel ledit disque optique (701, 100) possède une structure par secteurs comprenant une pluralité de secteurs, dans lesquels chacun des secteurs (401) comprend une zone d'en-tête de secteur (402) et une zone principale de données (403), comprenant les étapes consistant à :

reproduire les données de contenu à partir d'une zone principale de données d'un secteur ;
juger, en se basant sur les données de contenu reproduites, si les données de contenu sont ou non cryptées ;
reproduire un index de clé à partir d'une zone (408) d'informations de clés de décryptage de la zone (402) d'en-tête de secteur du même secteur à partir duquel les données de contenu ont été reproduites par ledit premier moyen de reproduction quand il est jugé que lesdites données de contenu sont cryptées,
acquérir et reproduire une clé de décryptage à partir d'un tableau (505) de clés de décryptage d'une zone (107) d'informations de gestion de clés en se basant sur l'index de clé reproduit, et décrypter les données de contenu cryptées au moyen de ladite clé de décryptage.

*Fig.1*

FIRST PREFERRED EMBODIMENT

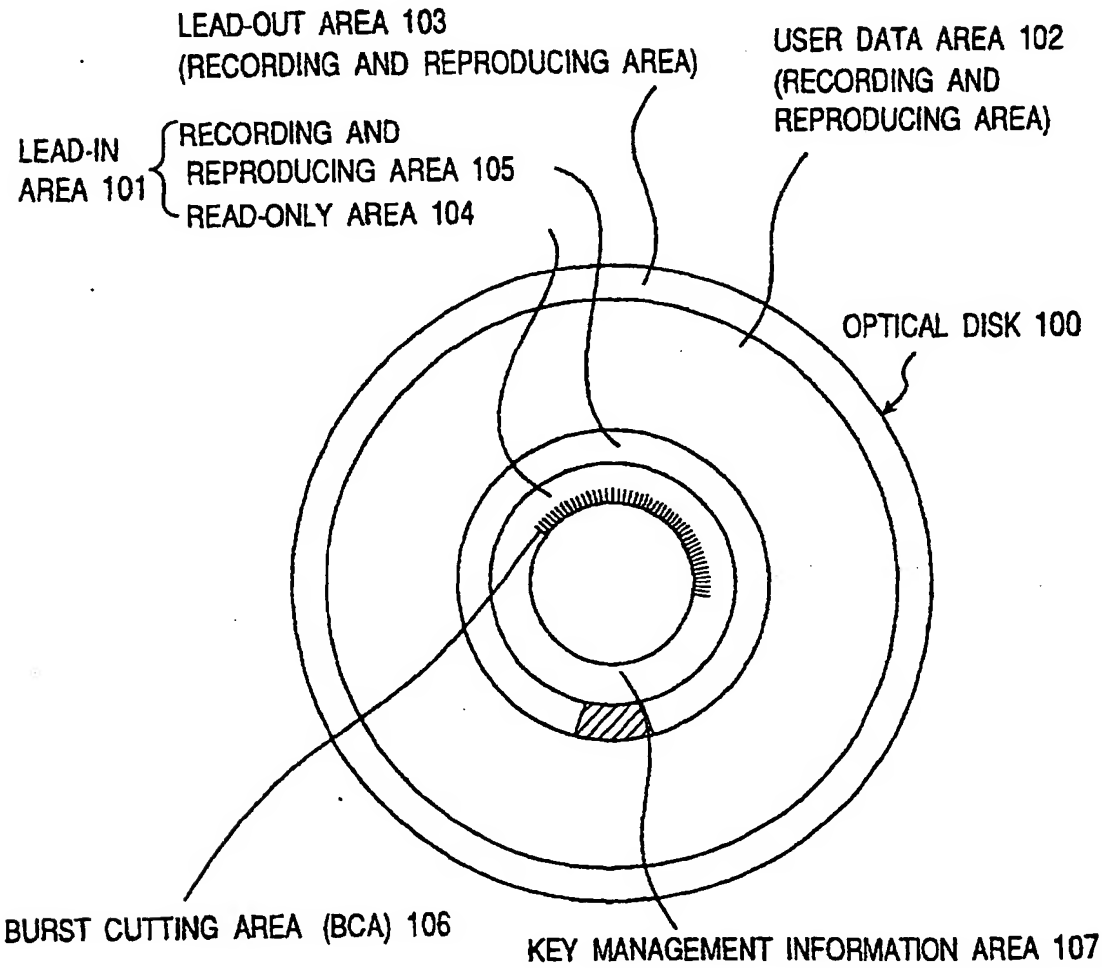


Fig.2A

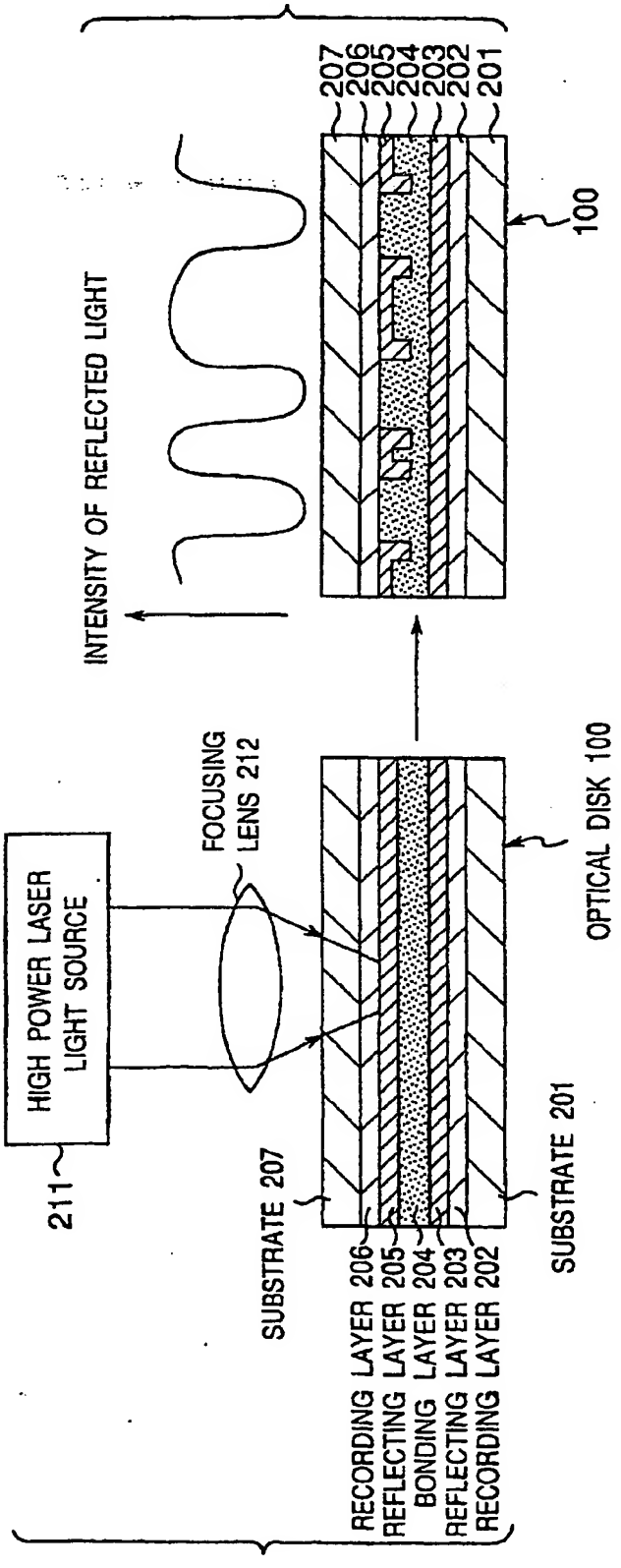

SECTIONAL VIEW OF OPTICAL DISK
(BEFORE FORMATION OF BCA)
HIGH POWER LASER
LIGHT SOURCE
211
FOCUSING
LENS 212
SUBSTRATE 207
RECORDING LAYER 206
REFLECTING LAYER 205
BONDING LAYER 204
REFLECTING LAYER 203
RECORDING LAYER 202
SUBSTRATE 201
OPTICAL DISK 100

Fig.2B


SECTIONAL VIEW OF OPTICAL DISK
(AFTER FORMATION OF BCA)
INTENSITY OF REFLECTED LIGHT
207
206
205
204
203
202
201
100

*Fig.3*

RECORDING FORMAT OF BCA 106

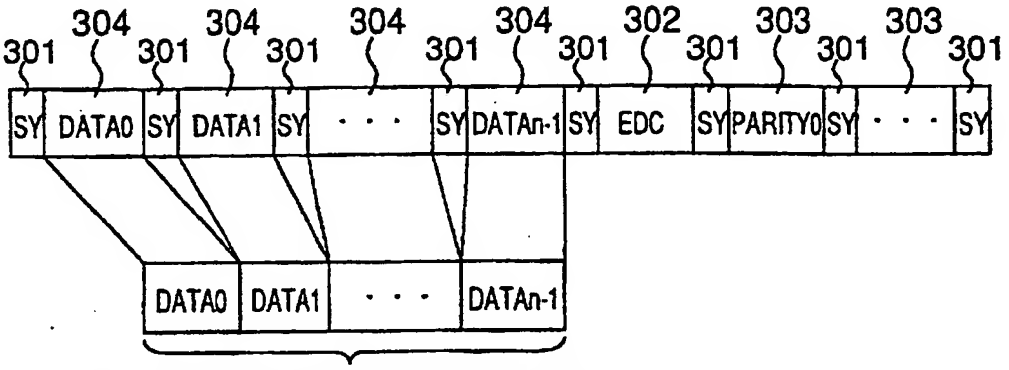



*Fig.4*

SECTOR STRUCTURE OF SECTOR DATA 401 IN USER DATA AREA 102

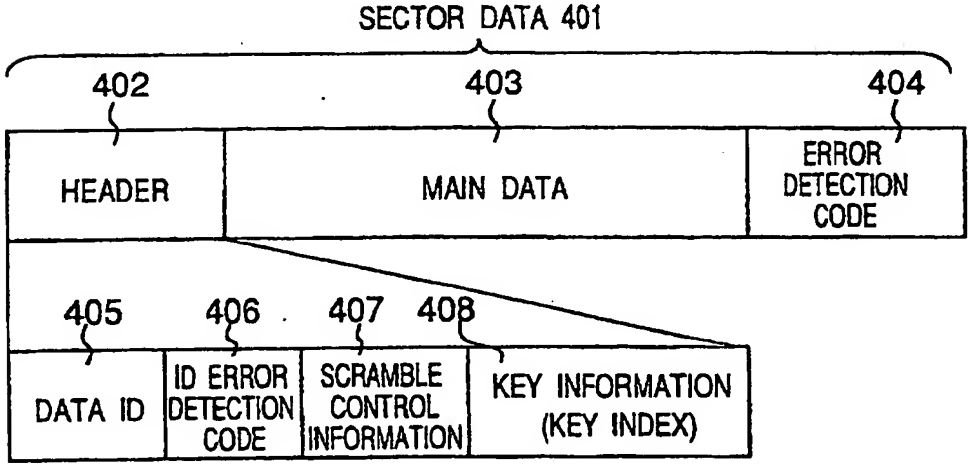


Fig.5

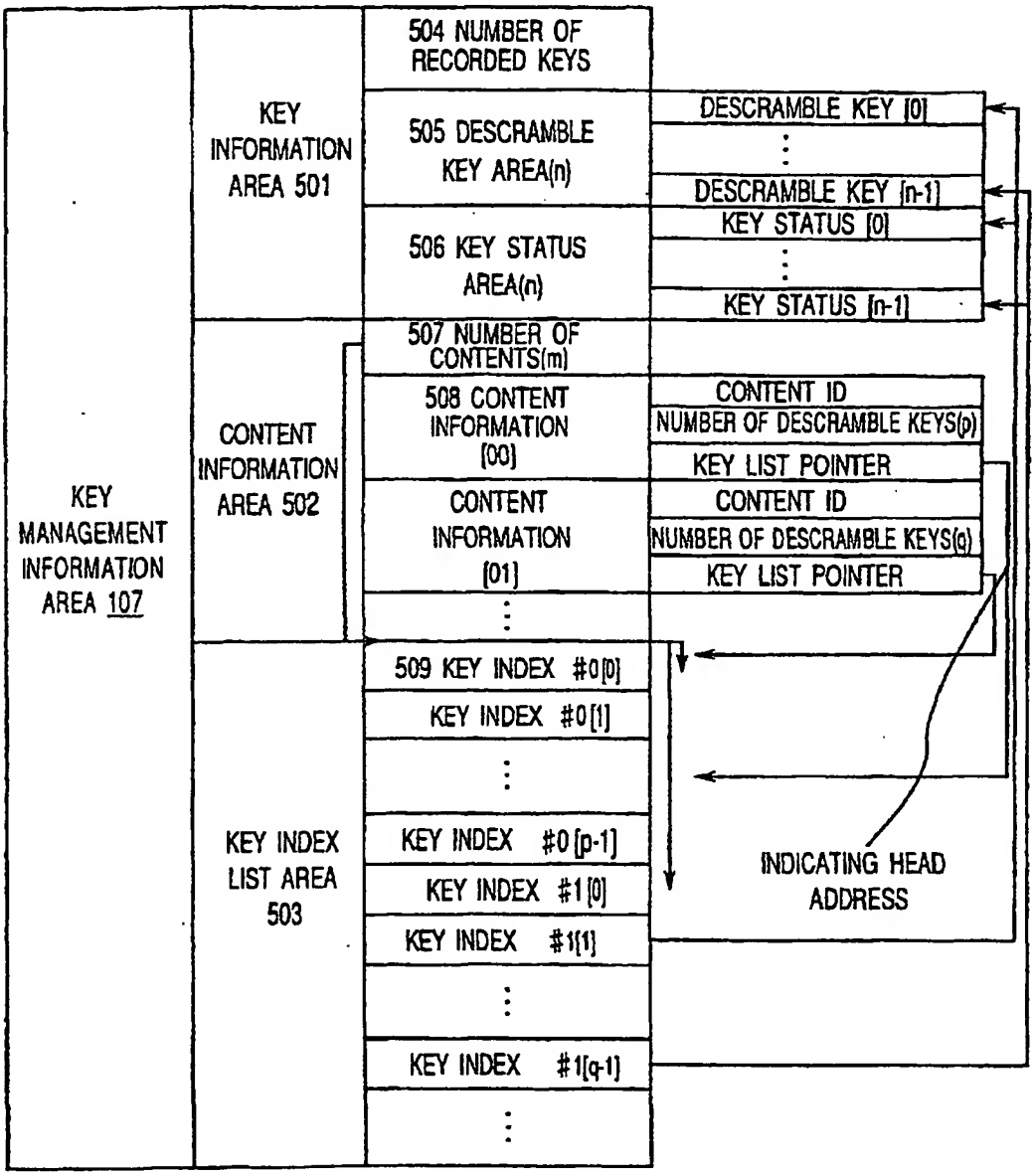

KEY MANAGEMENT INFORMATION AREA 107
KEY INFORMATION AREA 501
504 NUMBER OF RECORDED KEYS
505 DESCRAMBLE KEY AREA(n)
DESCRAMBLE KEY [0]
DESCRAMBLE KEY [n-1]
506 KEY STATUS AREA(n)
KEY STATUS [0]
KEY STATUS [n-1]
CONTENT INFORMATION AREA 502
507 NUMBER OF CONTENTS(m)
508 CONTENT INFORMATION [00]
CONTENT ID
NUMBER OF DESCRAMBLE KEYS(p)
KEY LIST POINTER
CONTENT INFORMATION [01]
CONTENT ID
NUMBER OF DESCRAMBLE KEYS(q)
KEY LIST POINTER
KEY INDEX LIST AREA 503
509 KEY INDEX #0[0]
KEY INDEX #0[1]
KEY INDEX #0[p-1]
KEY INDEX #1[0]
KEY INDEX #1[1]
KEY INDEX #1[q-1]
INDICATING HEAD ADDRESS

*Fig.6A*

CASE WHERE DESCRAMBLE KEY IS RECORDED IN SECTOR DATA 401 (MODIFIED FIRST PREFERRED EMBODIMENT)

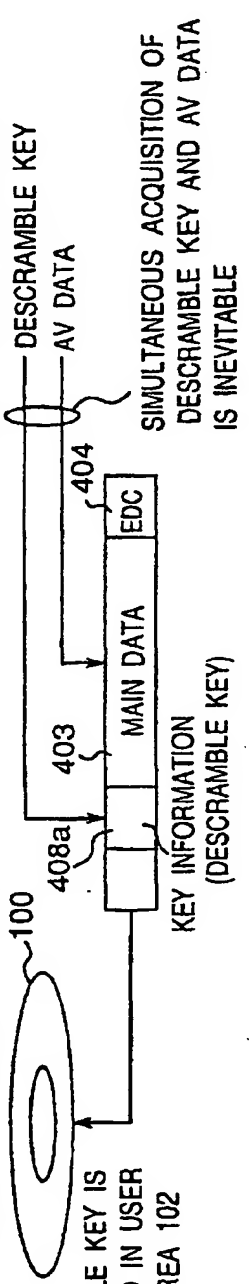



*Fig.6B*

CASE WHERE KEY INDEX TO DESCRAMBLE KEY IS RECORDED IN SECTOR DATA 401 (FIRST PREFERRED EMBODIMENT)

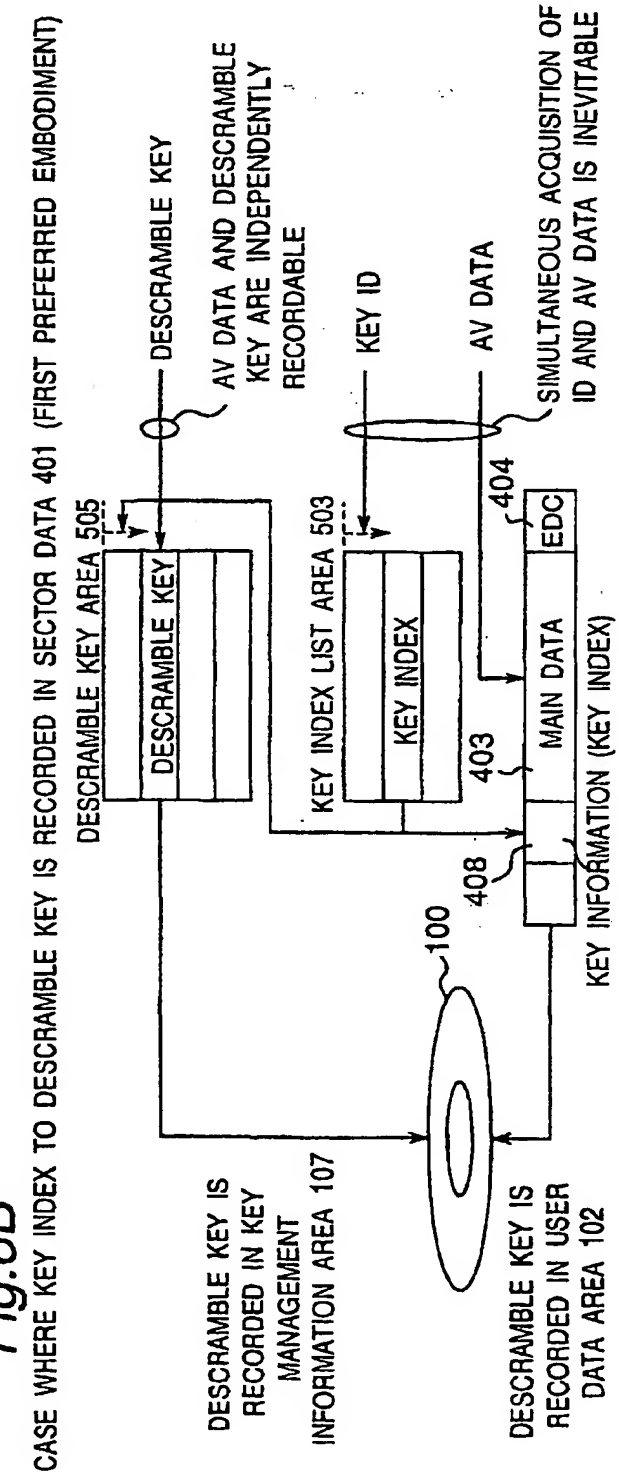


Fig.7

SECOND PREFERRED EMBODIMENT
OPTICAL DISK RECORDING AND REPRODUCING APPARATUS

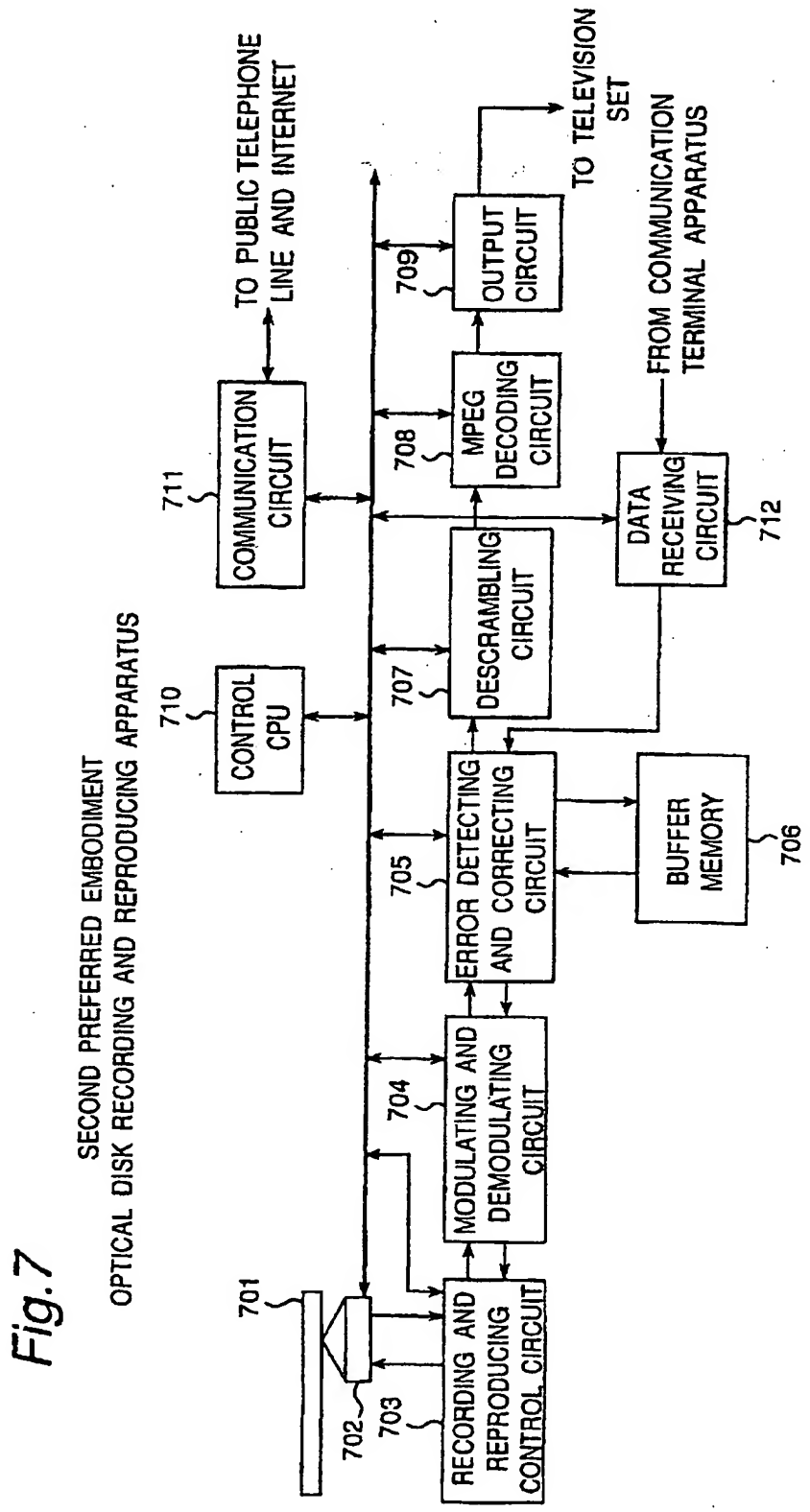


*Fig.8*

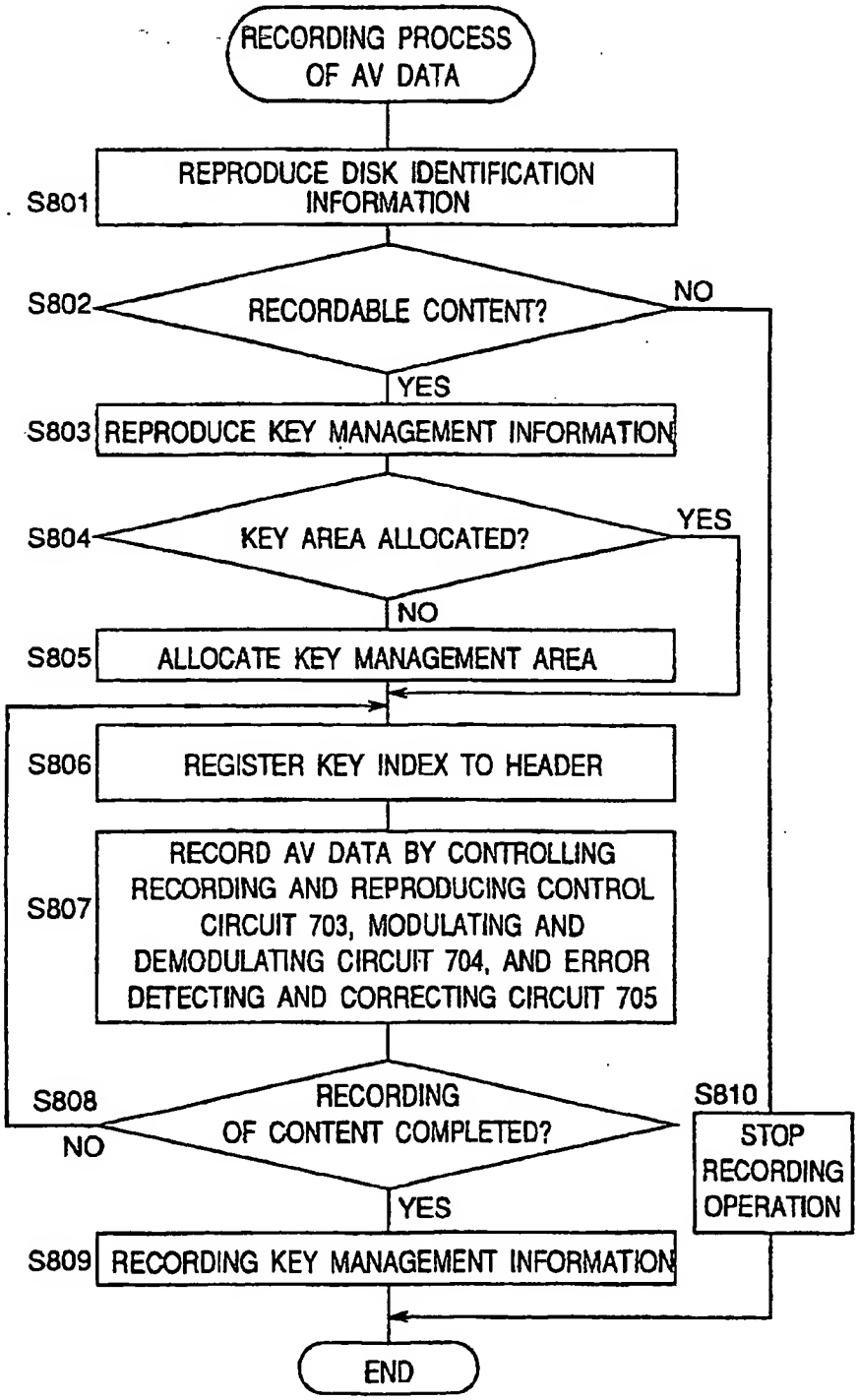

RECORDING PROCESS OF AV DATA
S801
REPRODUCE DISK IDENTIFICATION INFORMATION
S802
RECORDABLE CONTENT?
NO
YES
S803
REPRODUCE KEY MANAGEMENT INFORMATION
S804
KEY AREA ALLOCATED?
YES
NO
S805
ALLOCATE KEY MANAGEMENT AREA
S806
REGISTER KEY INDEX TO HEADER
S807
RECORD AV DATA BY CONTROLLING RECORDING AND REPRODUCING CONTROL CIRCUIT 703, MODULATING AND DEMODULATING CIRCUIT 704, AND ERROR DETECTING AND CORRECTING CIRCUIT 705
S808
RECORDING OF CONTENT COMPLETED?
NO
YES
S809
RECORDING KEY MANAGEMENT INFORMATION
S810
STOP RECORDING OPERATION
END

Fig.9

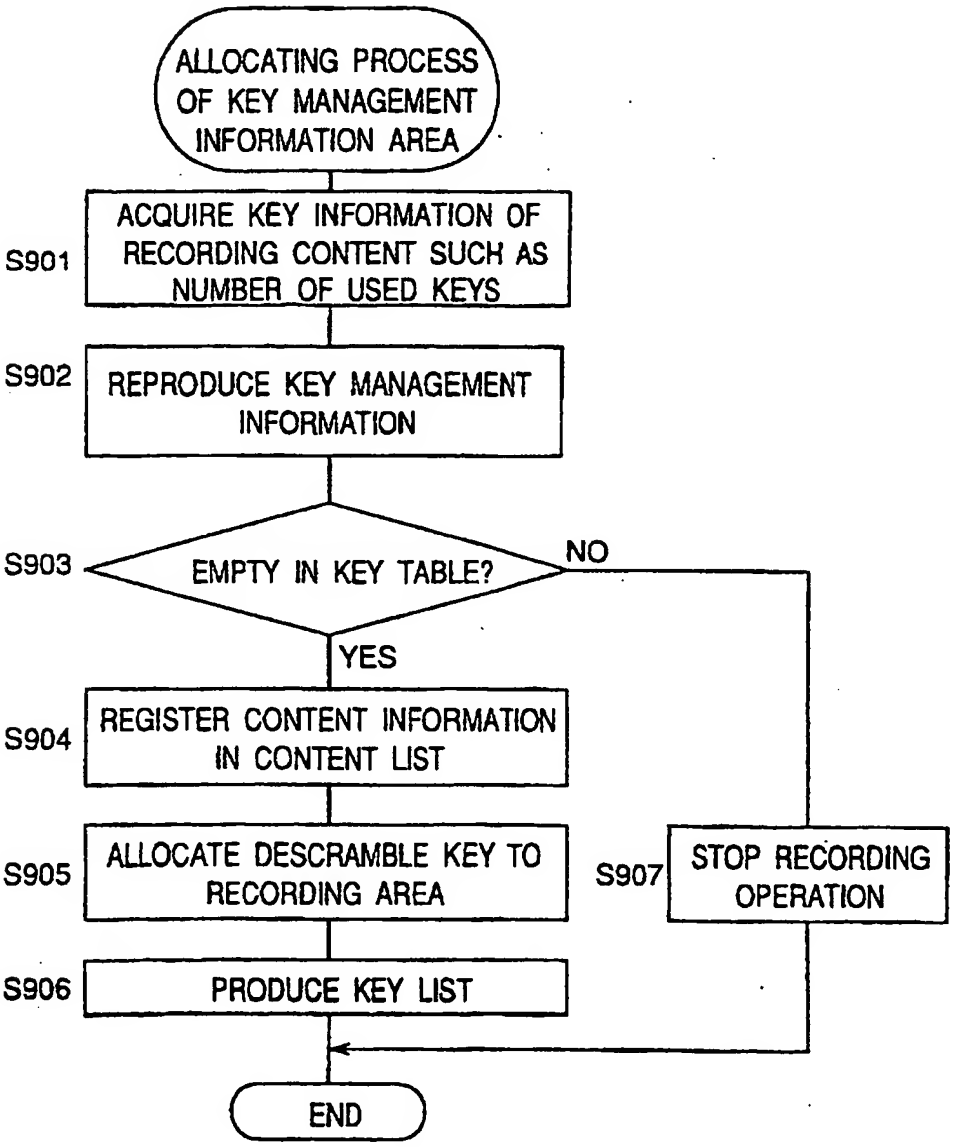

ALLOCATING PROCESS OF KEY MANAGEMENT INFORMATION AREA
S901
ACQUIRE KEY INFORMATION OF RECORDING CONTENT SUCH AS NUMBER OF USED KEYS
S902
REPRODUCE KEY MANAGEMENT INFORMATION
S903
EMPTY IN KEY TABLE?
NO
YES
S904
REGISTER CONTENT INFORMATION IN CONTENT LIST
S905
ALLOCATE DESCRAMBLE KEY TO RECORDING AREA
S906
PRODUCE KEY LIST
S907
STOP RECORDING OPERATION
END

Fig.10

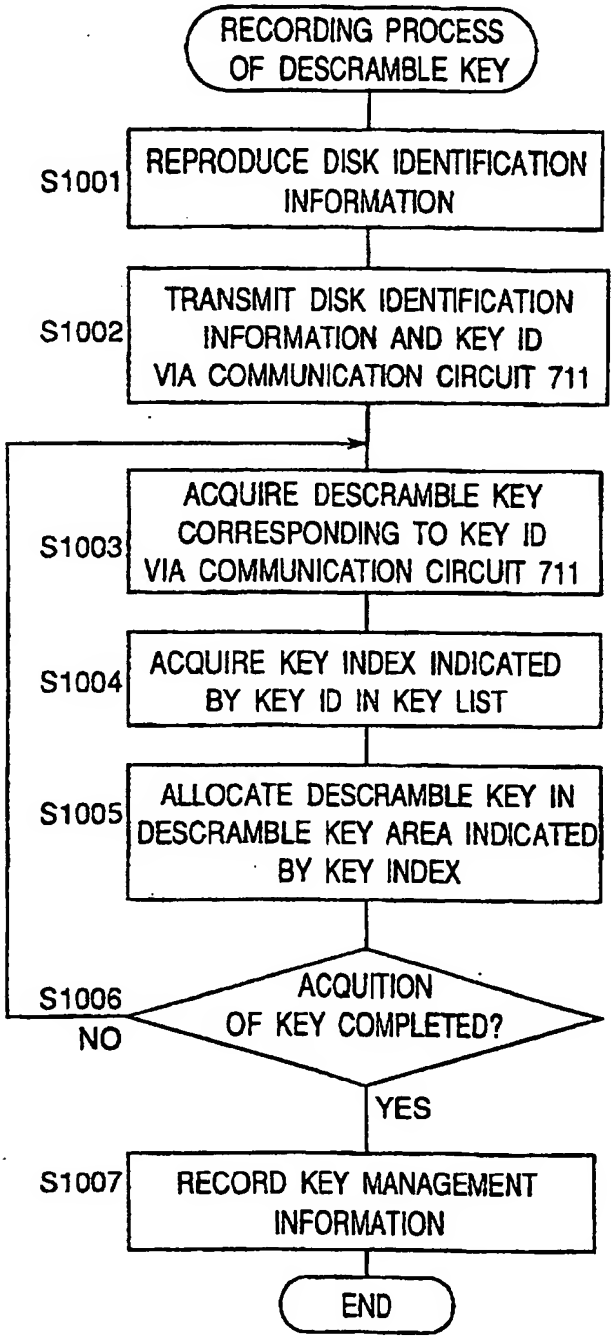

RECORDING PROCESS OF DESCRAMBLE KEY
S1001
REPRODUCE DISK IDENTIFICATION INFORMATION
S1002
TRANSMIT DISK IDENTIFICATION INFORMATION AND KEY ID VIA COMMUNICATION CIRCUIT 711
S1003
ACQUIRE DESCRAMBLE KEY CORRESPONDING TO KEY ID VIA COMMUNICATION CIRCUIT 711
S1004
ACQUIRE KEY INDEX INDICATED BY KEY ID IN KEY LIST
S1005
ALLOCATE DESCRAMBLE KEY IN DESCRAMBLE KEY AREA INDICATED BY KEY INDEX
S1006
ACQUITION OF KEY COMPLETED?
NO
YES
S1007
RECORD KEY MANAGEMENT INFORMATION
END

Fig.11

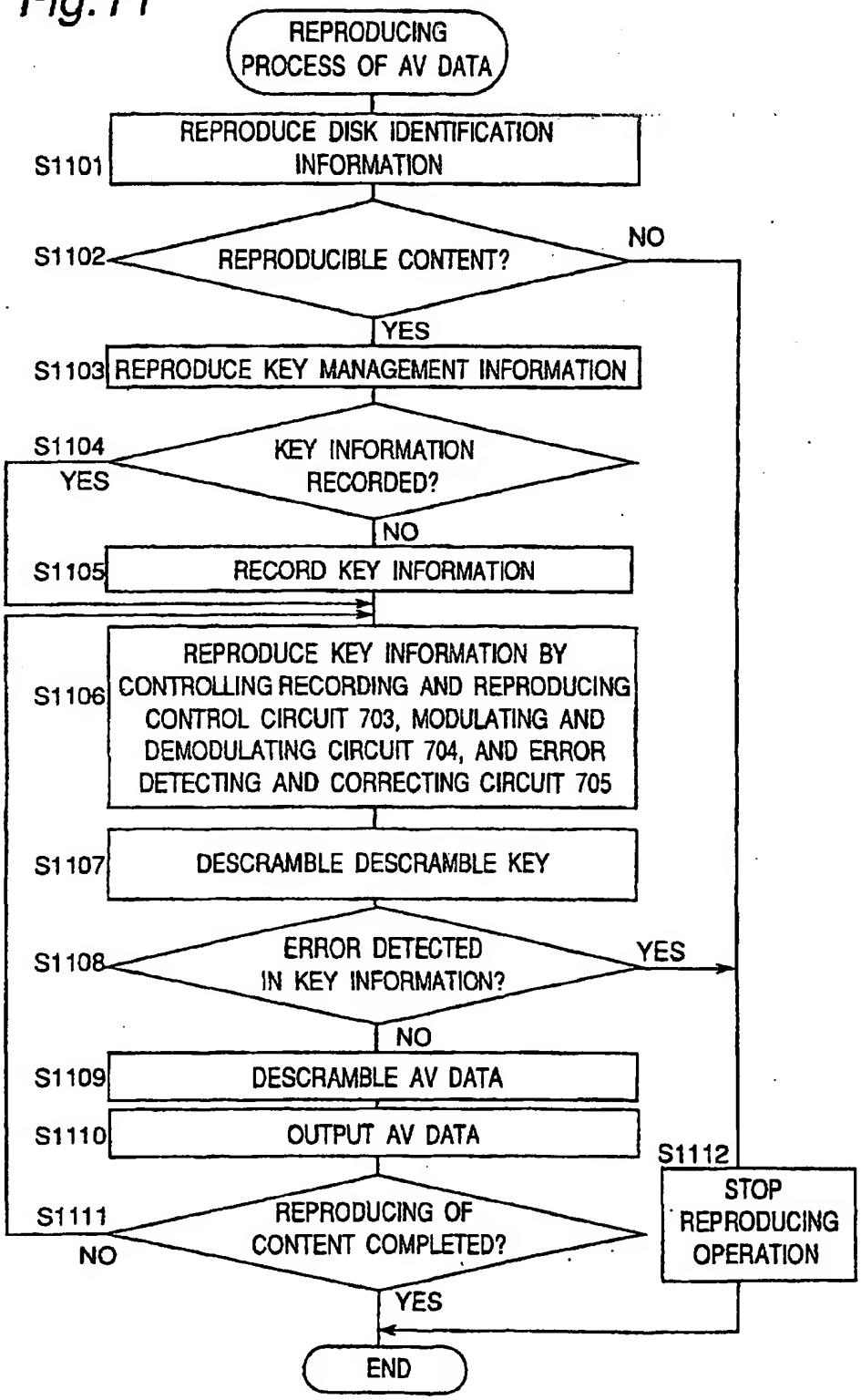

REPRODUCING PROCESS OF AV DATA
S1101
REPRODUCE DISK IDENTIFICATION INFORMATION
S1102
REPRODUCIBLE CONTENT?
NO
YES
S1103
REPRODUCE KEY MANAGEMENT INFORMATION
S1104
KEY INFORMATION RECORDED?
YES
NO
S1105
RECORD KEY INFORMATION
S1106
REPRODUCE KEY INFORMATION BY CONTROLLING RECORDING AND REPRODUCING CONTROL CIRCUIT 703, MODULATING AND DEMODULATING CIRCUIT 704, AND ERROR DETECTING AND CORRECTING CIRCUIT 705
S1107
DESCRAMBLE DESCRAMBLE KEY
S1108
ERROR DETECTED IN KEY INFORMATION?
YES
NO
S1109
DESCRAMBLE AV DATA
S1110
OUTPUT AV DATA
S1111
REPRODUCING OF CONTENT COMPLETED?
NO
YES
S1112
STOP REPRODUCING OPERATION
END

Fig.12

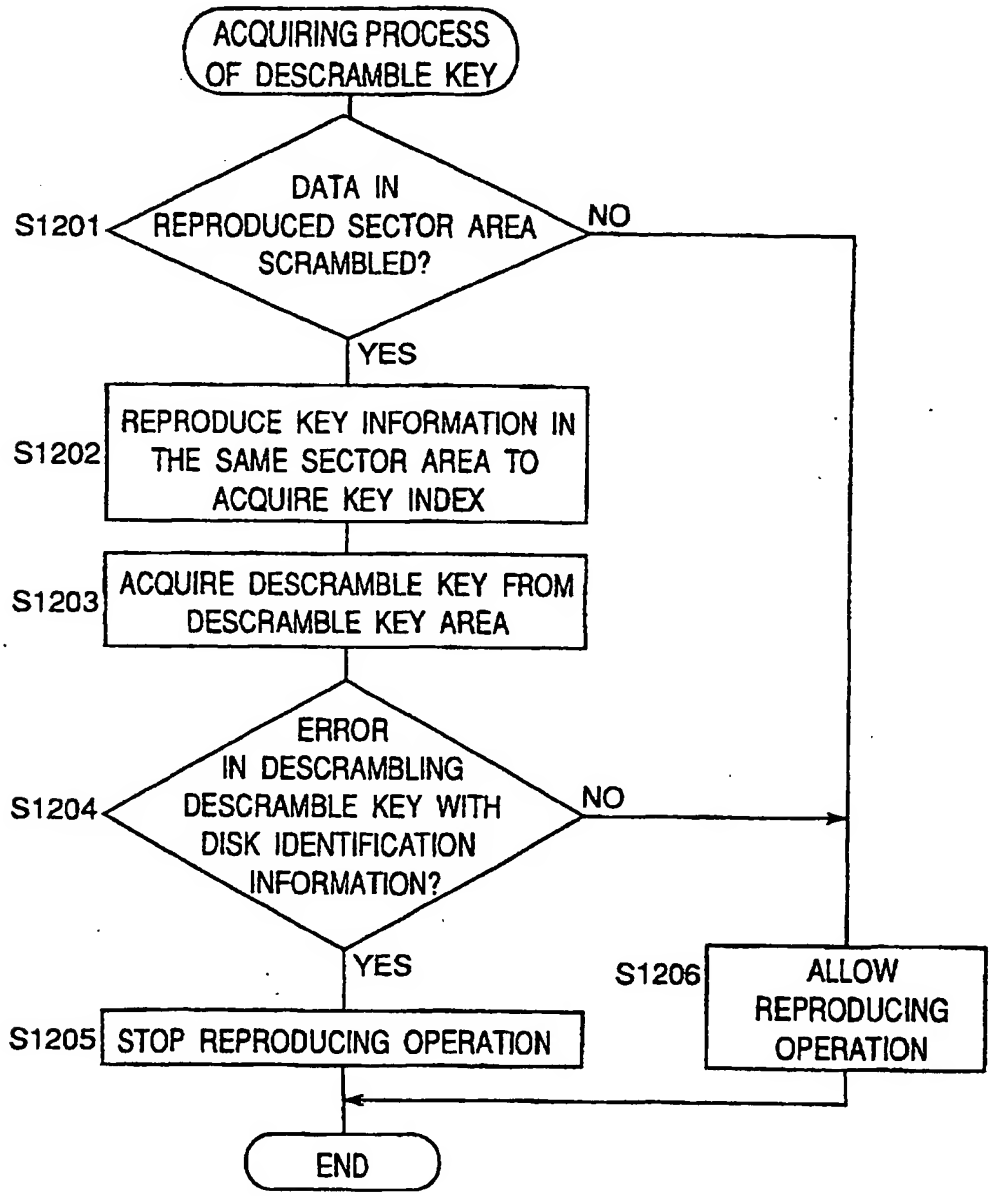

ACQUIRING PROCESS OF DESCRAMBLE KEY
S1201
DATA IN REPRODUCED SECTOR AREA SCRAMBLED?
NO
YES
S1202
REPRODUCE KEY INFORMATION IN THE SAME SECTOR AREA TO ACQUIRE KEY INDEX
S1203
ACQUIRE DESCRAMBLE KEY FROM DESCRAMBLE KEY AREA
S1204
ERROR IN DESCRAMBLING DESCRAMBLE KEY WITH DISK IDENTIFICATION INFORMATION?
NO
YES
S1205
STOP REPRODUCING OPERATION
S1206
ALLOW REPRODUCING OPERATION
END

Fig.13

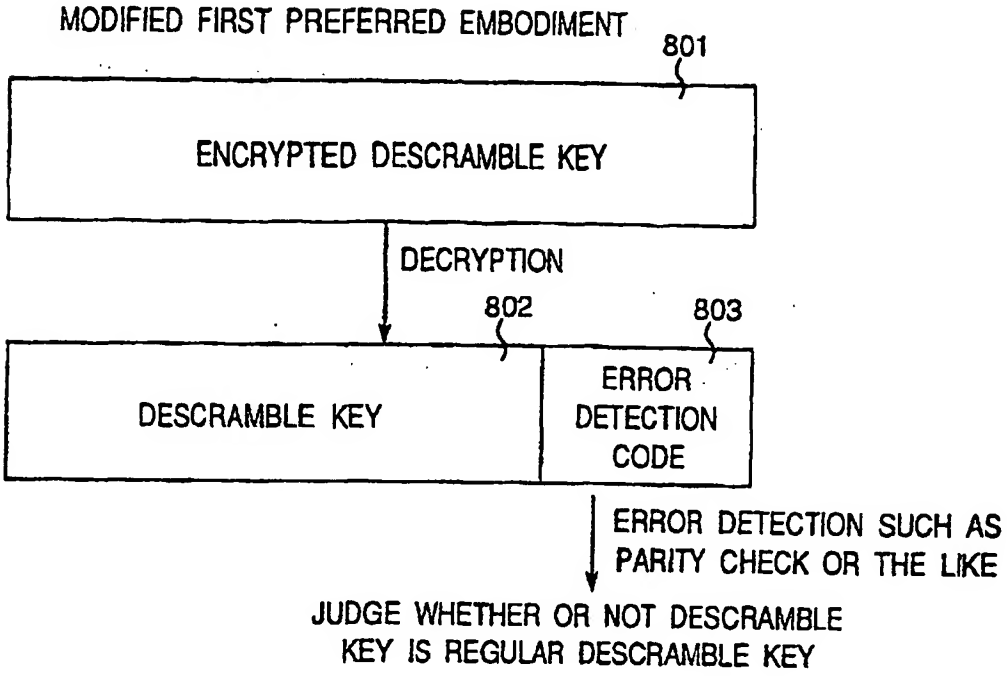



Fig.14

MODIFIED FIRST PREFERRED EMBODIMENT

DESCRAMBLE AREA MANAGEMENT TABLE

| | | | |
|---|---|---|---|
| 1 | START ADDRESS 1 | END ADDRESS 1 | DESCRAMBLE KEY 1 |
| 2 | START ADDRESS 2 | END ADDRESS 2 | DESCRAMBLE KEY 2 |
| ⋮ | ⋮ | ⋮ | ⋮ |
| n | START ADDRESS n | END ADDRESS n | DESCRAMBLE KEY n |

Fig.15A

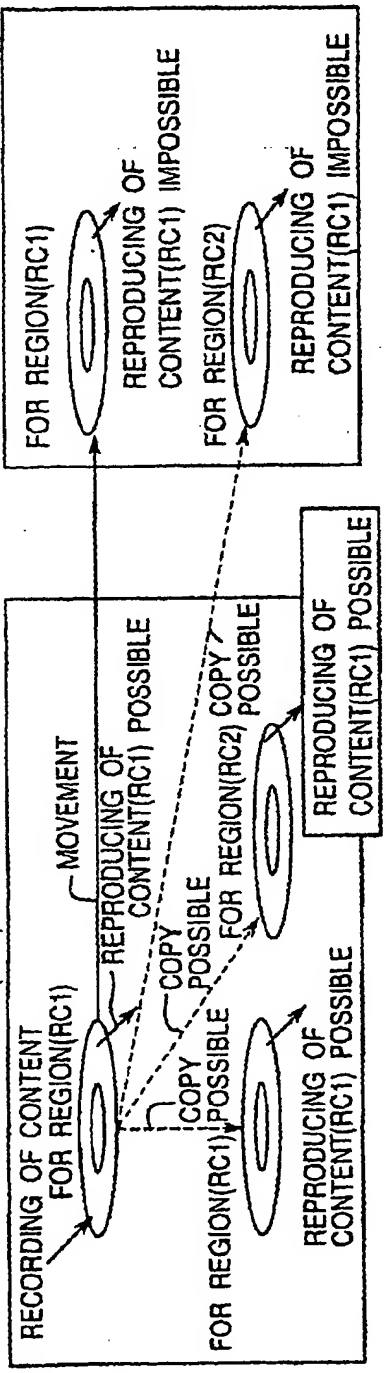



Fig.15B

*Fig.16*

THIRD PREFERRED EMBODIMENT

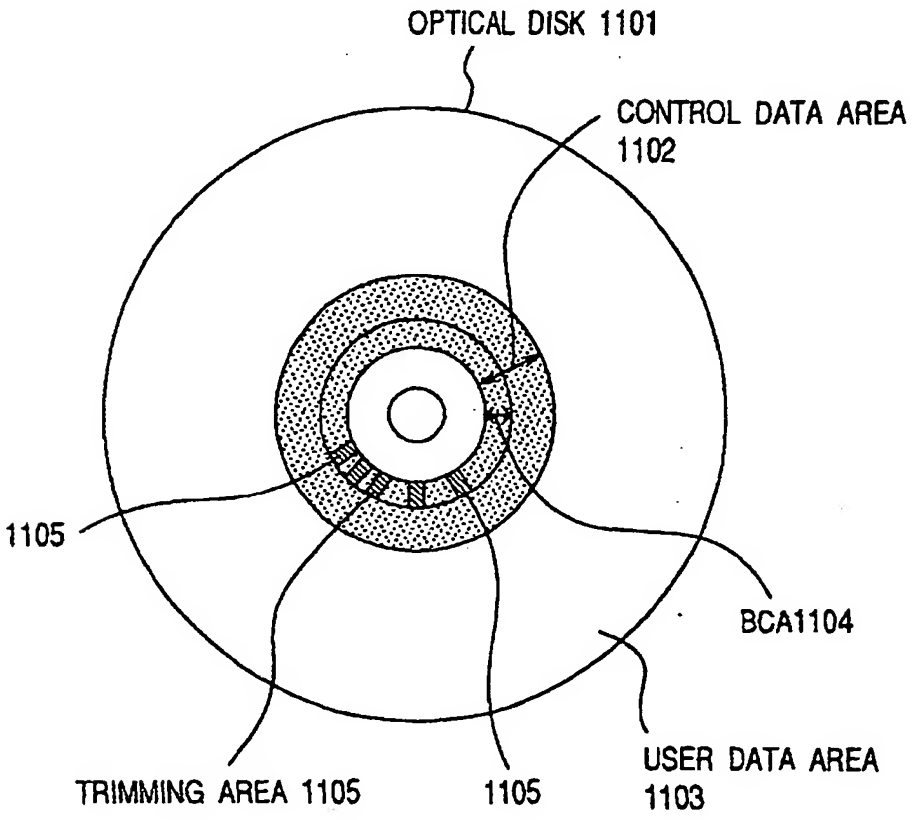


Fig.17

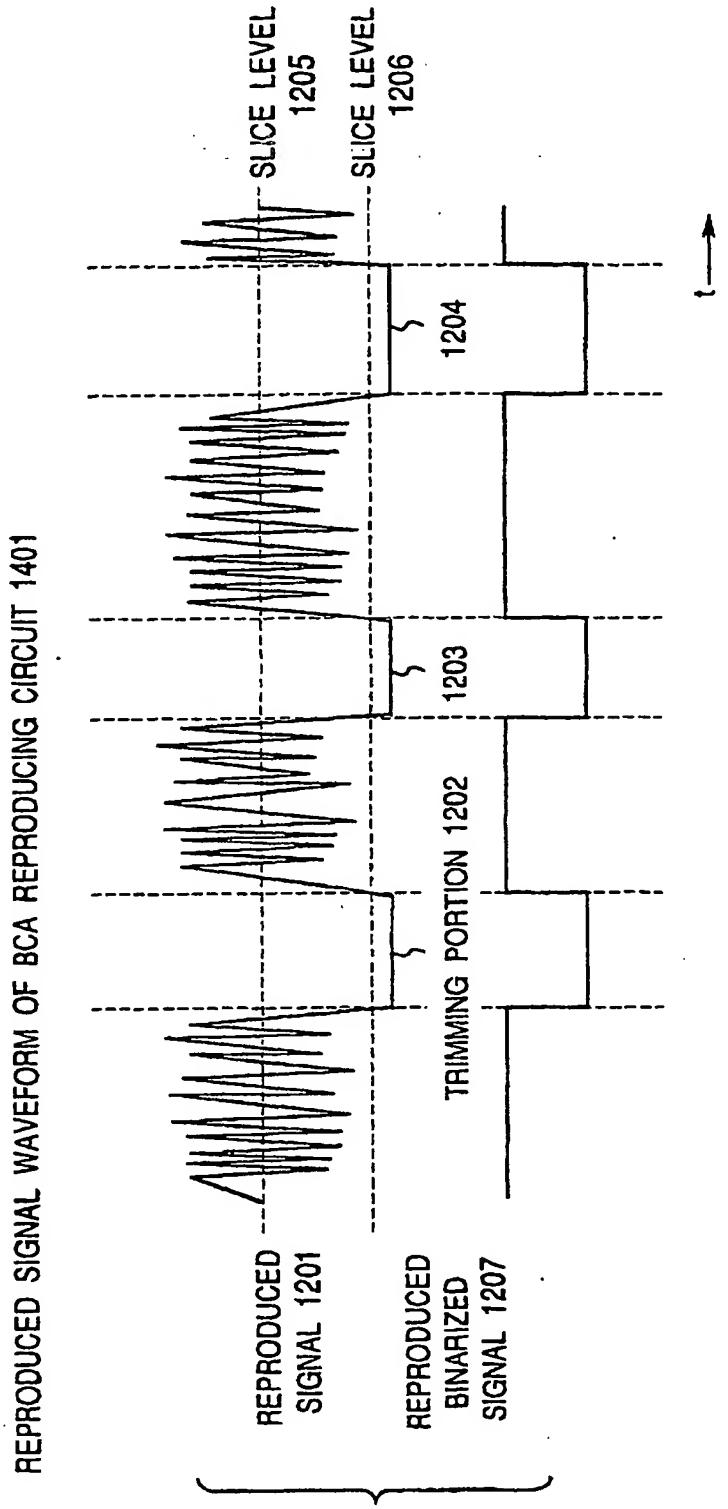

REPRODUCED SIGNAL WAVEFORM OF BCA REPRODUCING CIRCUIT 1401
SLICE LEVEL 1205
SLICE LEVEL 1206
1204
1203
TRIMMING PORTION 1202
t
REPRODUCED SIGNAL 1201
REPRODUCED BINARIZED SIGNAL 1207

Fig.18

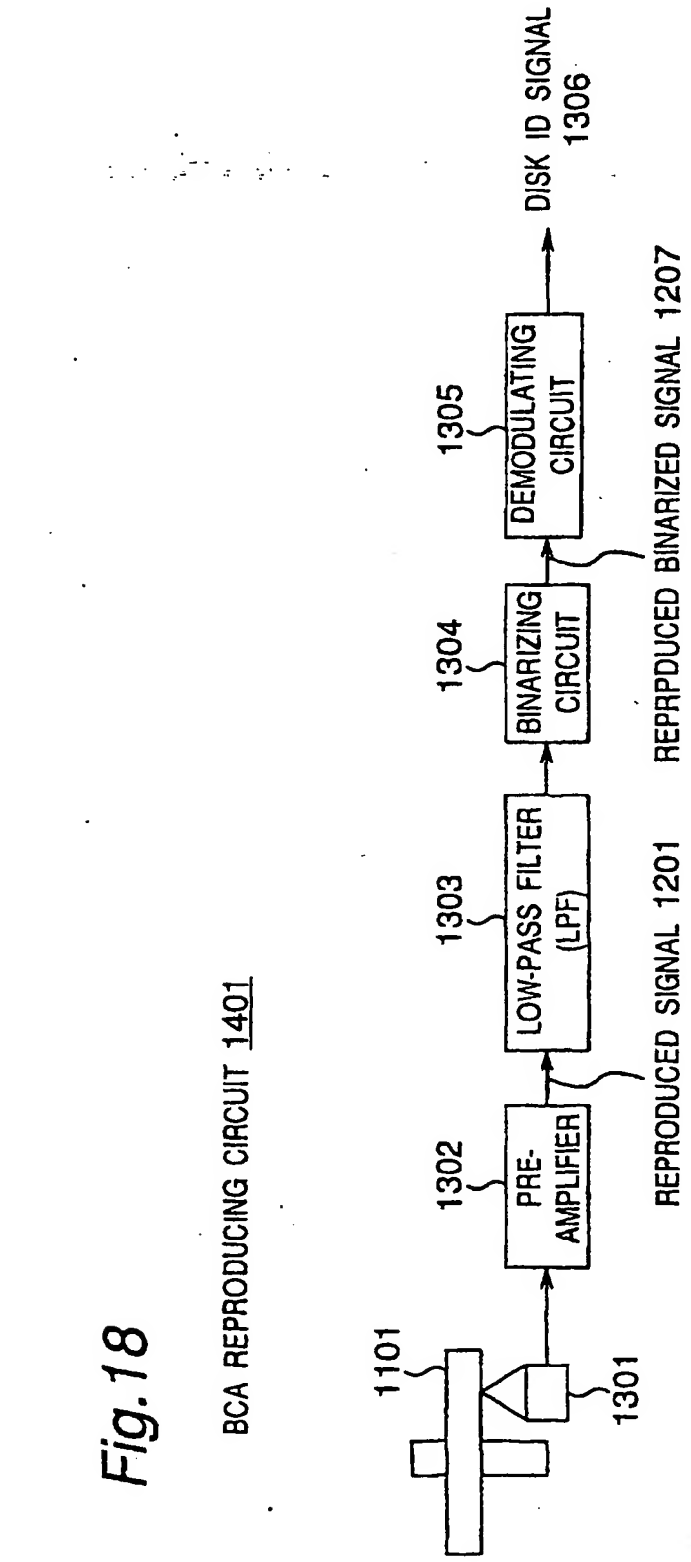

BCA REPRODUCING CIRCUIT 1401
1101
1301
1302
PRE-AMPLIFIER
REPRODUCED SIGNAL 1201
1303
LOW-PASS FILTER (LPF)
1304
BINARIZING CIRCUIT
REPRPDUCED BINARIZED SIGNAL 1207
1305
DEMODULATING CIRCUIT
DISK ID SIGNAL 1306

Fig.19

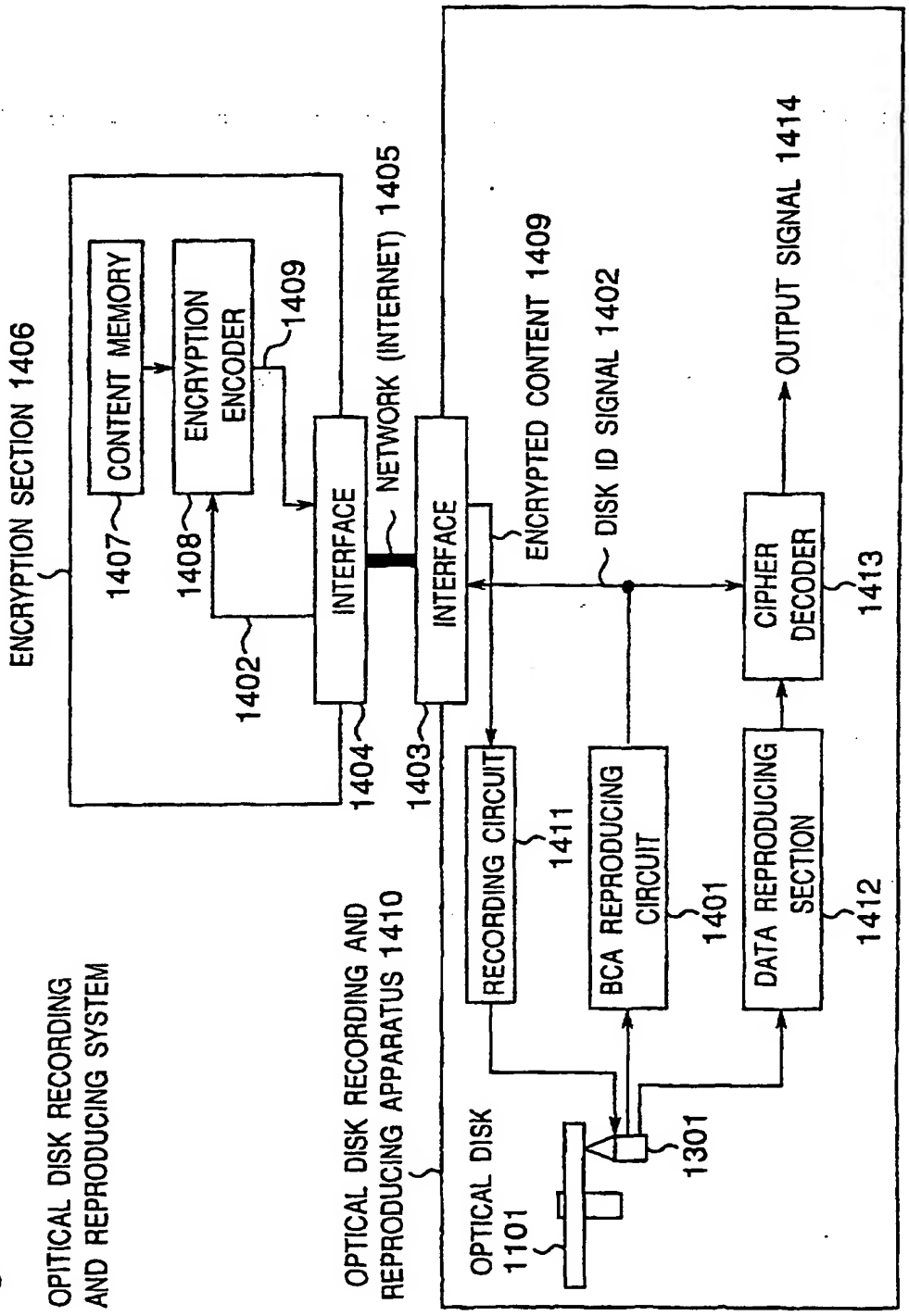

OPTICAL DISK RECORDING AND REPRODUCING SYSTEM
OPTICAL DISK RECORDING AND REPRODUCING APPARATUS 1410
ENCRYPTION SECTION 1406
CONTENT MEMORY
1407
ENCRYPTION ENCODER
1408
1409
1402
INTERFACE
1404
NETWORK (INTERNET) 1405
INTERFACE
1403
ENCRYPTED CONTENT 1409
DISK ID SIGNAL 1402
OUTPUT SIGNAL 1414
RECORDING CIRCUIT
1411
BCA REPRODUCING CIRCUIT
1401
DATA REPRODUCING SECTION
1412
CIPHER DECODER
1413
OPTICAL DISK 1101
1301

Fig.20

FOURTH PREFERRED EMBODIMENT
OPTICAL DISK RECORDING AND REPRODUCING SYSTEM

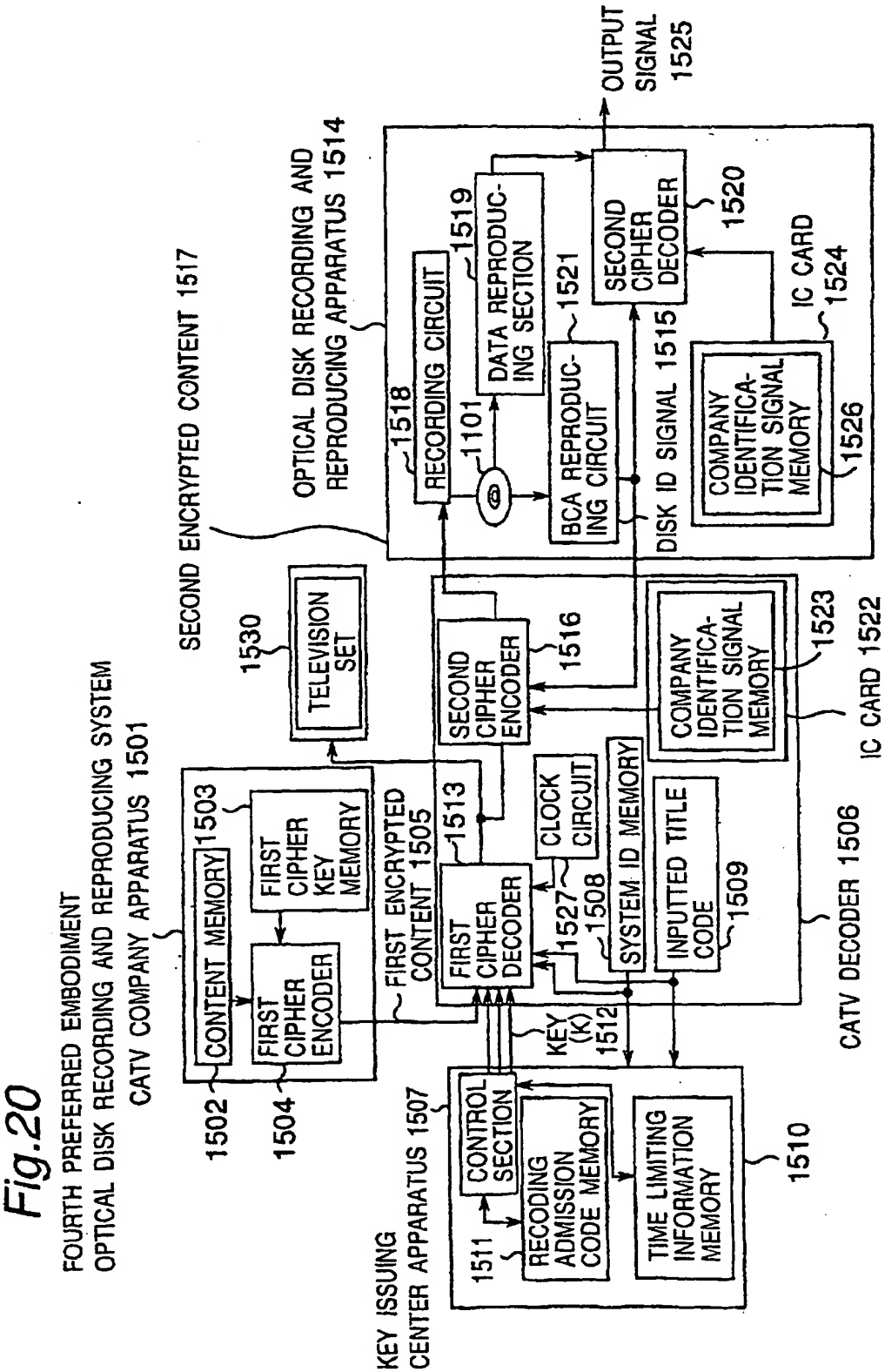


*Fig.21*

FIFTH PREFERRED EMBODIMENT

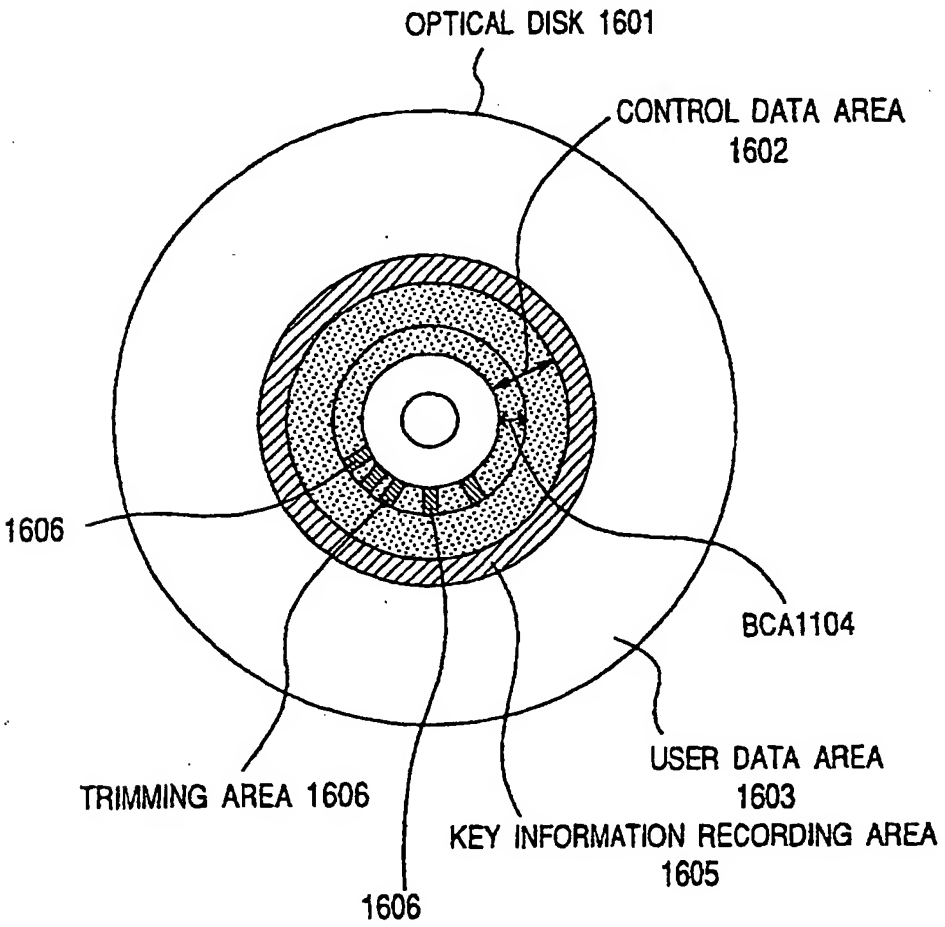


Fig.22

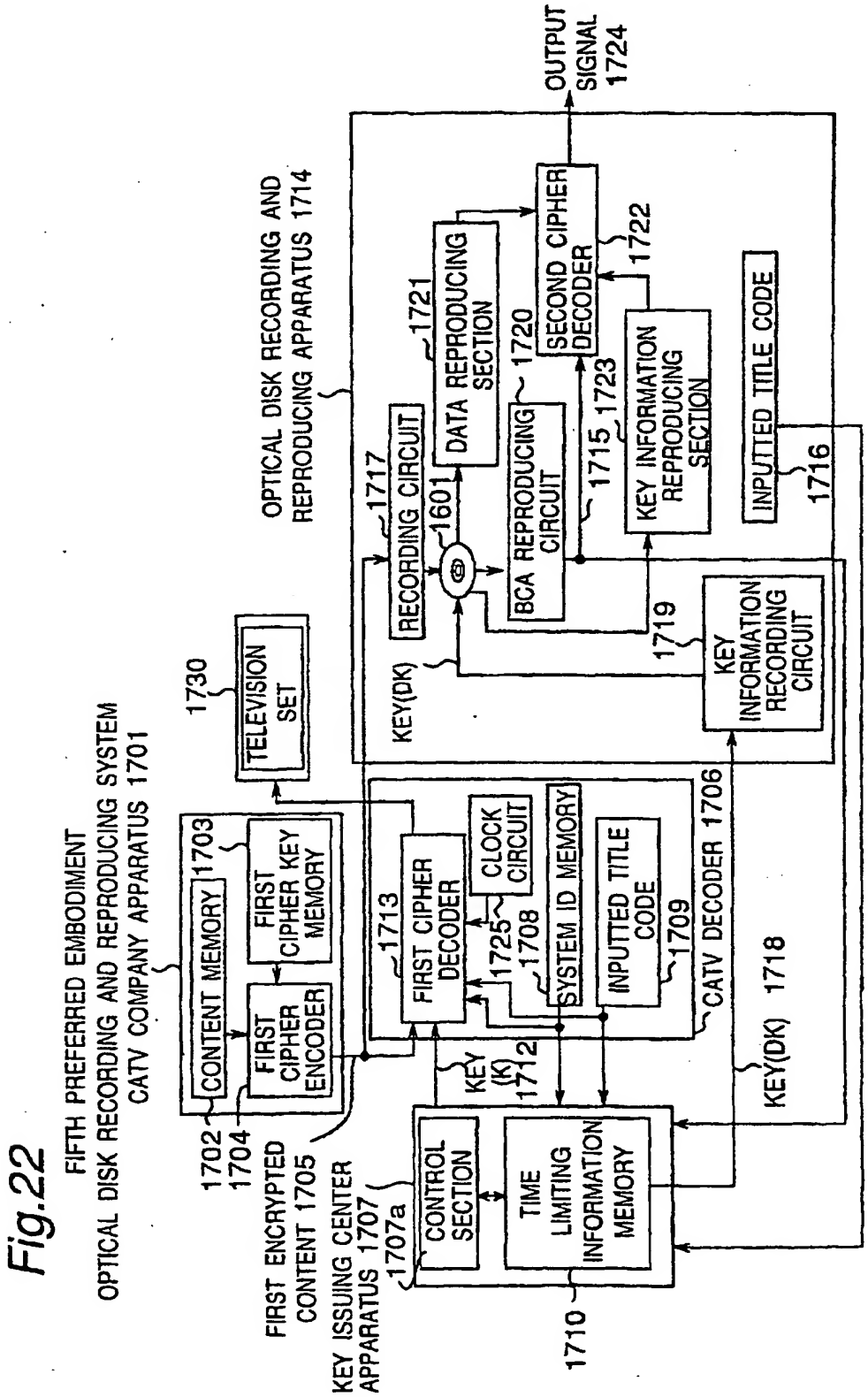

FIFTH PREFERRED EMBODIMENT
OPTICAL DISK RECORDING AND REPRODUCING SYSTEM
CATV COMPANY APPARATUS 1701
OPTICAL DISK RECORDING AND REPRODUCING APPARATUS 1714
OUTPUT SIGNAL 1724
TELEVISION SET
1730
CONTENT MEMORY
1703
FIRST CIPHER KEY MEMORY
FIRST CIPHER ENCODER
1702
1704
FIRST ENCRYPTED CONTENT 1705
KEY ISSUING CENTER APPARATUS 1707
1707a
CONTROL SECTION
TIME LIMITING INFORMATION MEMORY
1710
KEY (K) 1712
FIRST CIPHER DECODER
1713
CLOCK CIRCUIT
1725
1708
SYSTEM ID MEMORY
INPUTTED TITLE CODE
1709
CATV DECODER 1706
KEY(DK) 1718
KEY(DK)
RECORDING CIRCUIT
1717
1601
1719
KEY INFORMATION RECORDING CIRCUIT
DATA REPRODUCING SECTION
1721
1720
BCA REPRODUCING CIRCUIT
1715
1723
SECOND CIPHER DECODER
1722
KEY INFORMATION REPRODUCING SECTION
INPUTTED TITLE CODE
1716

Fig.23

TABLE WITH ID

| | | T1 | T2 | T3 |
|---|---|---|---|---|
| TITLE CODE T | | FK1 | FK2 | FK3 |
| FIRST DECIPHER KEY FK | | TIME1 | TIME2 | TIME3 |
| TIME LIMITING INFORMATION TIME | | K11 | K12 | K13 |
| SYSTEM ID | DID1 | K21 | K22 | K23 |
| | DID2 | K23 | K32 | K33 |
| | DID3 | DK11 | DK12 | DK13 |
| DISK ID | BCAS1 | DK21 | DK22 | DK23 |
| | BCAS2 | DK31 | DK32 | DK33 |
| | BCAS3 | | | |

*Fig.24*

MODIFIED THIRD PREFERRED EMBODIMENT

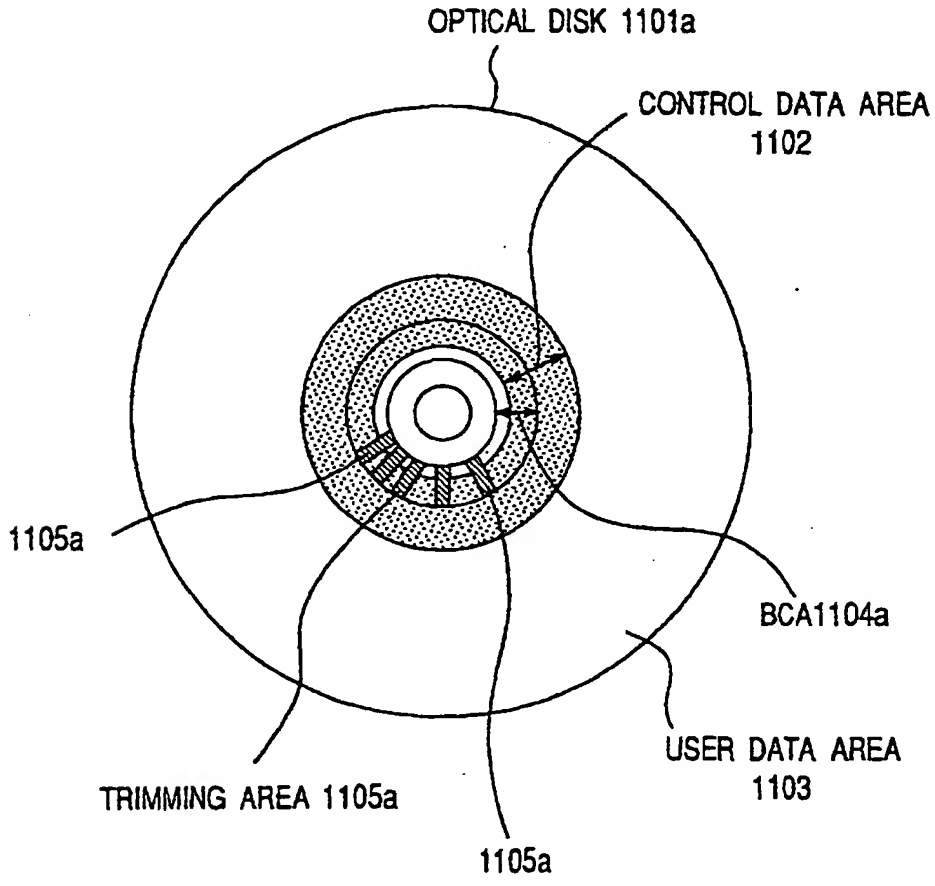


*Fig.25*

MODIFIED FIFTH PREFERRED EMBODIMENT

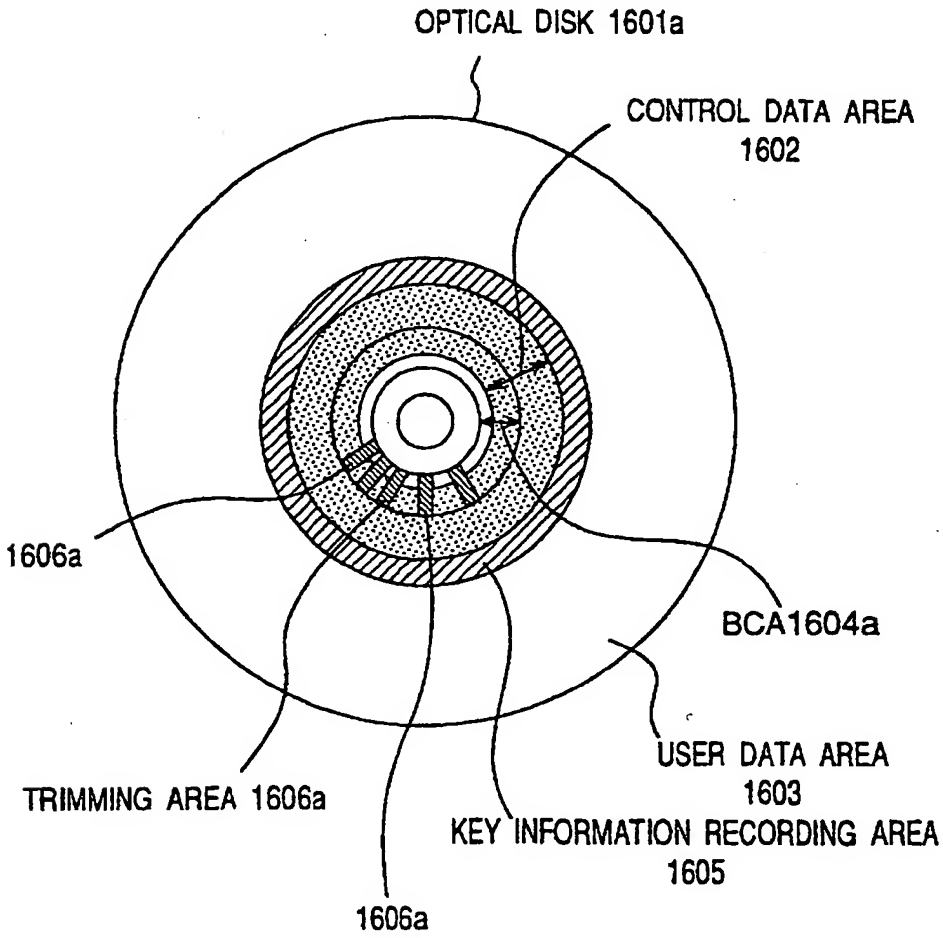


Fig.26

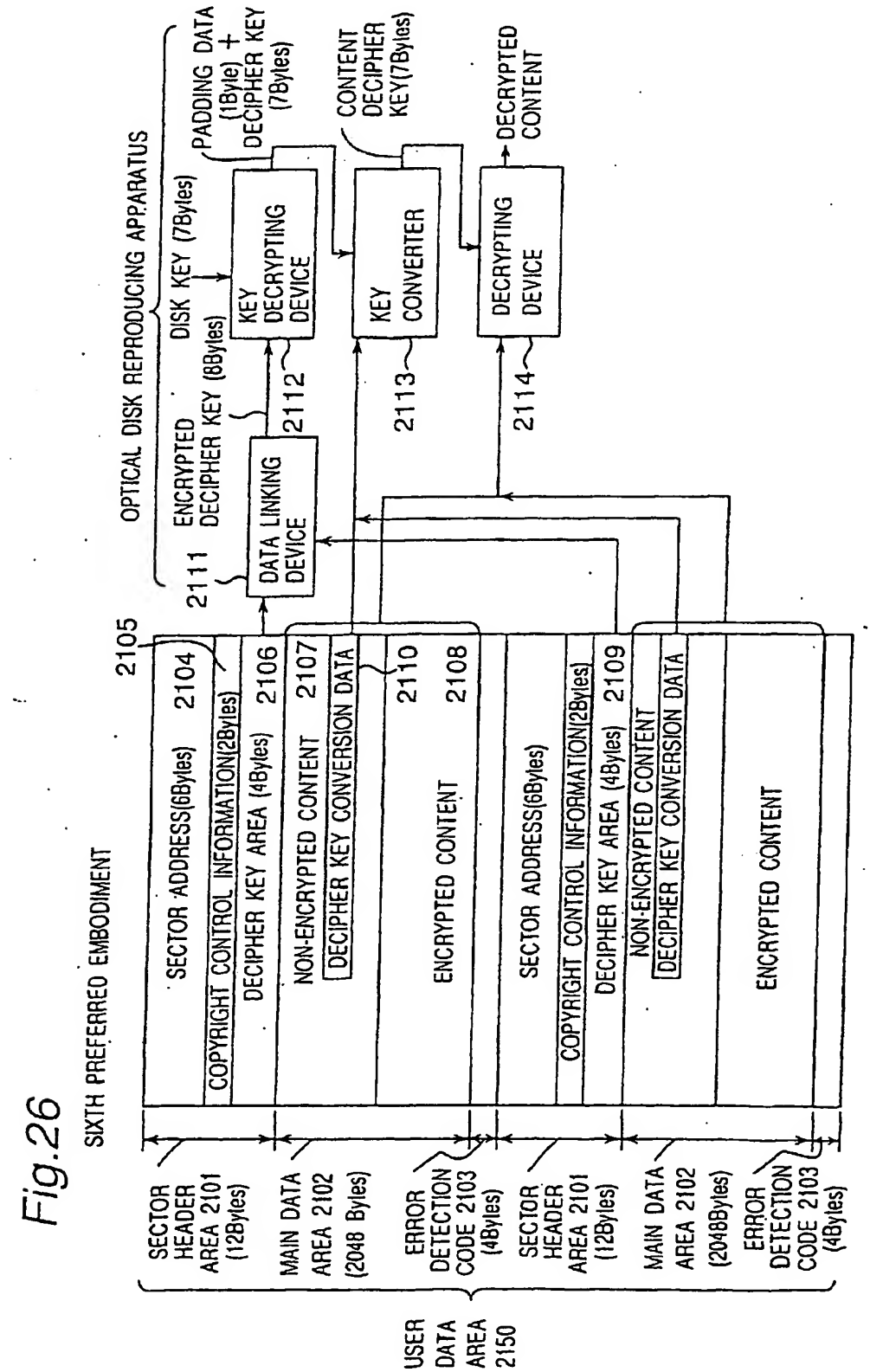

SIXTH PREFERRED EMBODIMENT
OPTICAL DISK REPRODUCING APPARATUS
2111
ENCRYPTED DECIPHER KEY (8Bytes)
DISK KEY (7Bytes)
DATA LINKING DEVICE
KEY DECRYPTING DEVICE
2112
PADDING DATA (1Byte) + DECIPHER KEY (7Bytes)
KEY CONVERTER
2113
CONTENT DECIPHER KEY(7Bytes)
DECRYPTING DEVICE
2114
DECRYPTED CONTENT
2105
SECTOR ADDRESS(6Bytes) 2104
COPYRIGHT CONTROL INFORMATION(2Bytes)
DECIPHER KEY AREA (4Bytes) 2106
NON-ENCRYPTED CONTENT 2107
DECIPHER KEY CONVERSION DATA
2110
ENCRYPTED CONTENT 2108
SECTOR ADDRESS(6Bytes)
COPYRIGHT CONTROL INFORMATION(2Bytes)
DECIPHER KEY AREA (4Bytes) 2109
NON-ENCRYPTED CONTENT
DECIPHER KEY CONVERSION DATA
ENCRYPTED CONTENT
SECTOR HEADER AREA 2101 (12Bytes)
MAIN DATA AREA 2102 (2048 Bytes)
ERROR DETECTION CODE 2103 (4Bytes)
SECTOR HEADER AREA 2101 (12Bytes)
MAIN DATA AREA 2102 (2048Bytes)
ERROR DETECTION CODE 2103 (4Bytes)
USER DATA AREA 2150

Fig.27

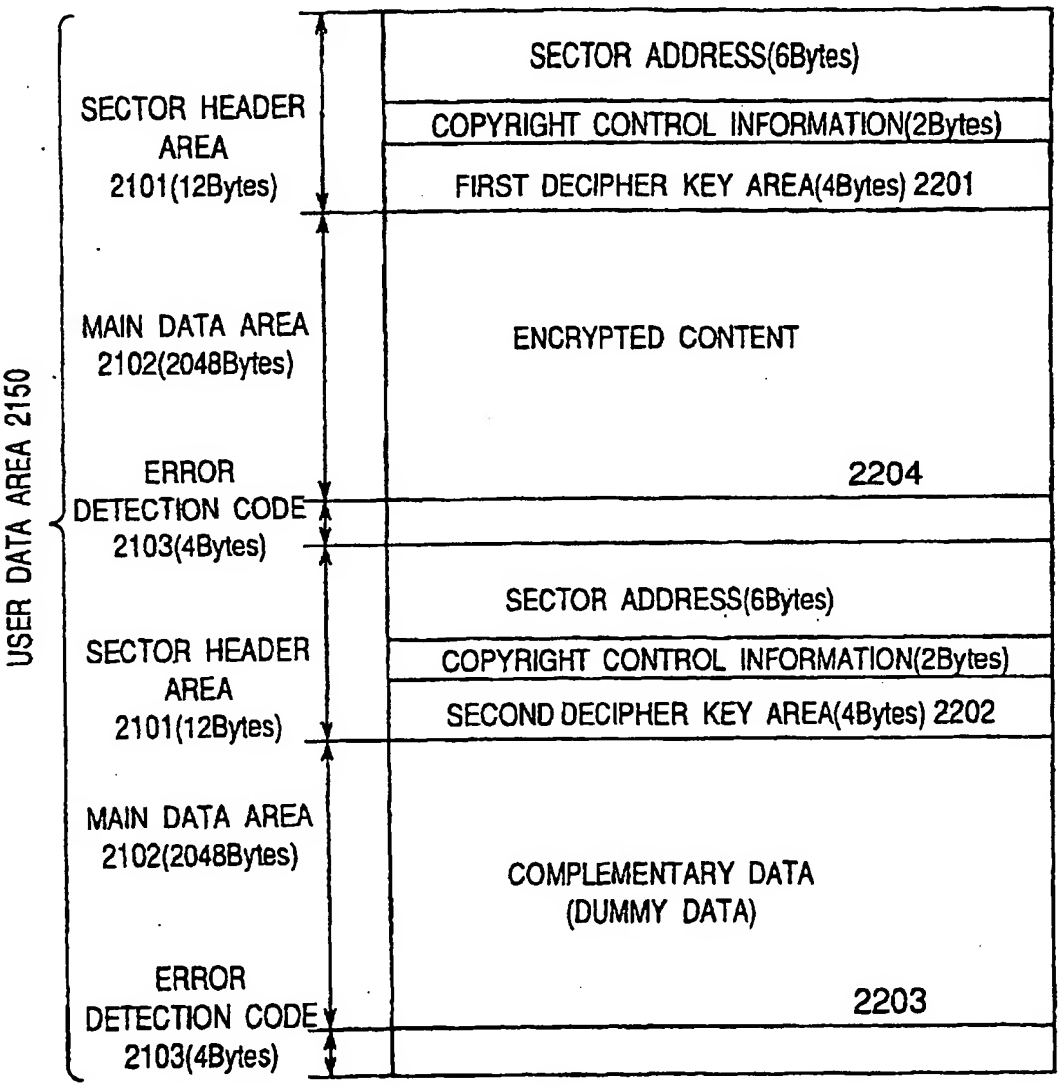

USER DATA AREA 2150
SECTOR HEADER AREA 2101(12Bytes)
SECTOR ADDRESS(6Bytes)
COPYRIGHT CONTROL INFORMATION(2Bytes)
FIRST DECIPHER KEY AREA(4Bytes) 2201
MAIN DATA AREA 2102(2048Bytes)
ENCRYPTED CONTENT
2204
ERROR DETECTION CODE 2103(4Bytes)
SECTOR HEADER AREA 2101(12Bytes)
SECTOR ADDRESS(6Bytes)
COPYRIGHT CONTROL INFORMATION(2Bytes)
SECOND DECIPHER KEY AREA(4Bytes) 2202
MAIN DATA AREA 2102(2048Bytes)
COMPLEMENTARY DATA (DUMMY DATA)
2203
ERROR DETECTION CODE 2103(4Bytes)

Fig.28

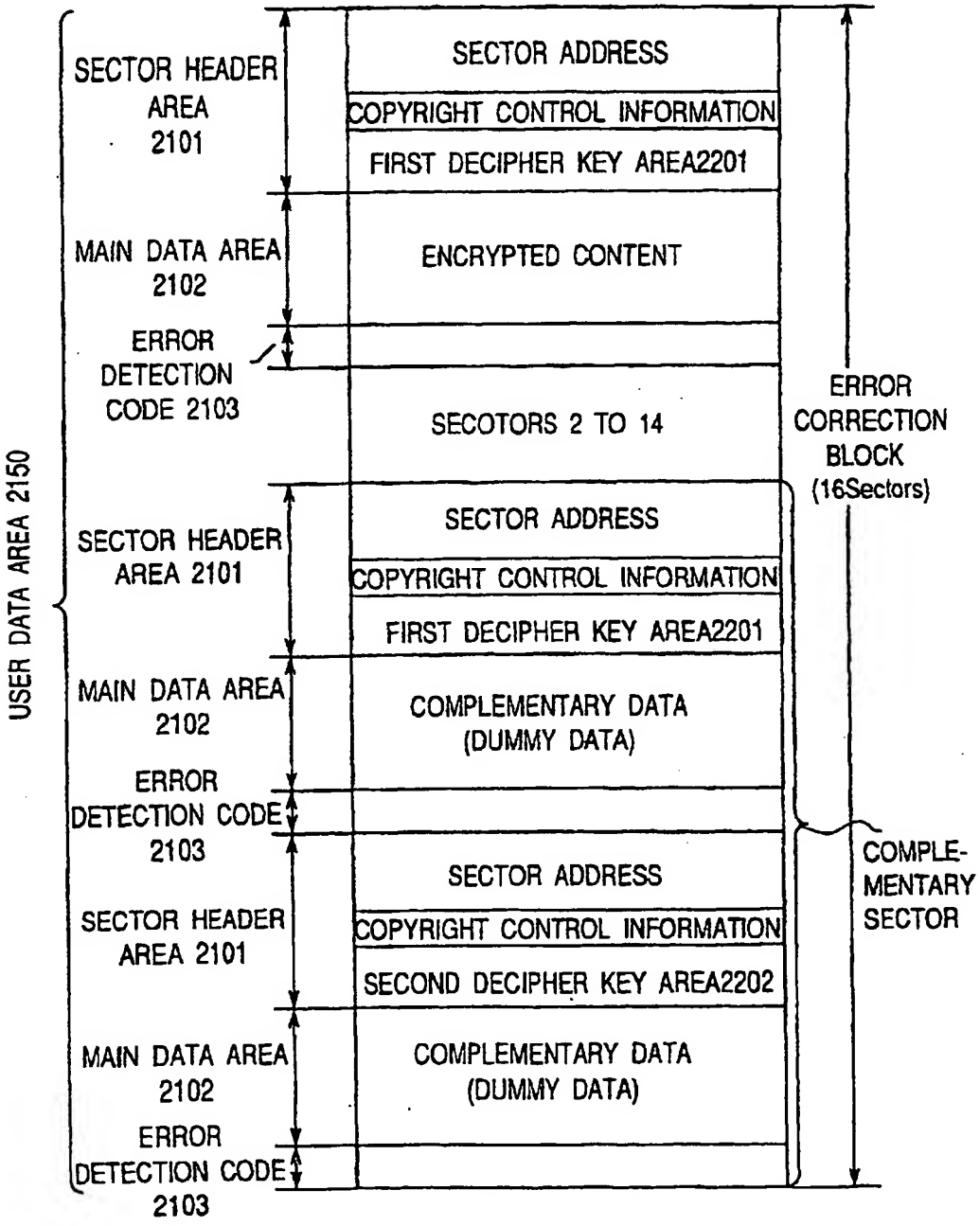

USER DATA AREA 2150
SECTOR HEADER AREA 2101
SECTOR ADDRESS
COPYRIGHT CONTROL INFORMATION
FIRST DECIPHER KEY AREA2201
MAIN DATA AREA 2102
ENCRYPTED CONTENT
ERROR DETECTION CODE 2103
SECOTORS 2 TO 14
ERROR CORRECTION BLOCK (16Sectors)
SECTOR HEADER AREA 2101
SECTOR ADDRESS
COPYRIGHT CONTROL INFORMATION
FIRST DECIPHER KEY AREA2201
MAIN DATA AREA 2102
COMPLEMENTARY DATA (DUMMY DATA)
ERROR DETECTION CODE 2103
SECTOR HEADER AREA 2101
SECTOR ADDRESS
COPYRIGHT CONTROL INFORMATION
SECOND DECIPHER KEY AREA2202
MAIN DATA AREA 2102
COMPLEMENTARY DATA (DUMMY DATA)
ERROR DETECTION CODE 2103
COMPLE-MENTARY SECTOR

Fig.29

SEVENTH PREFERRED EMBODIMENT

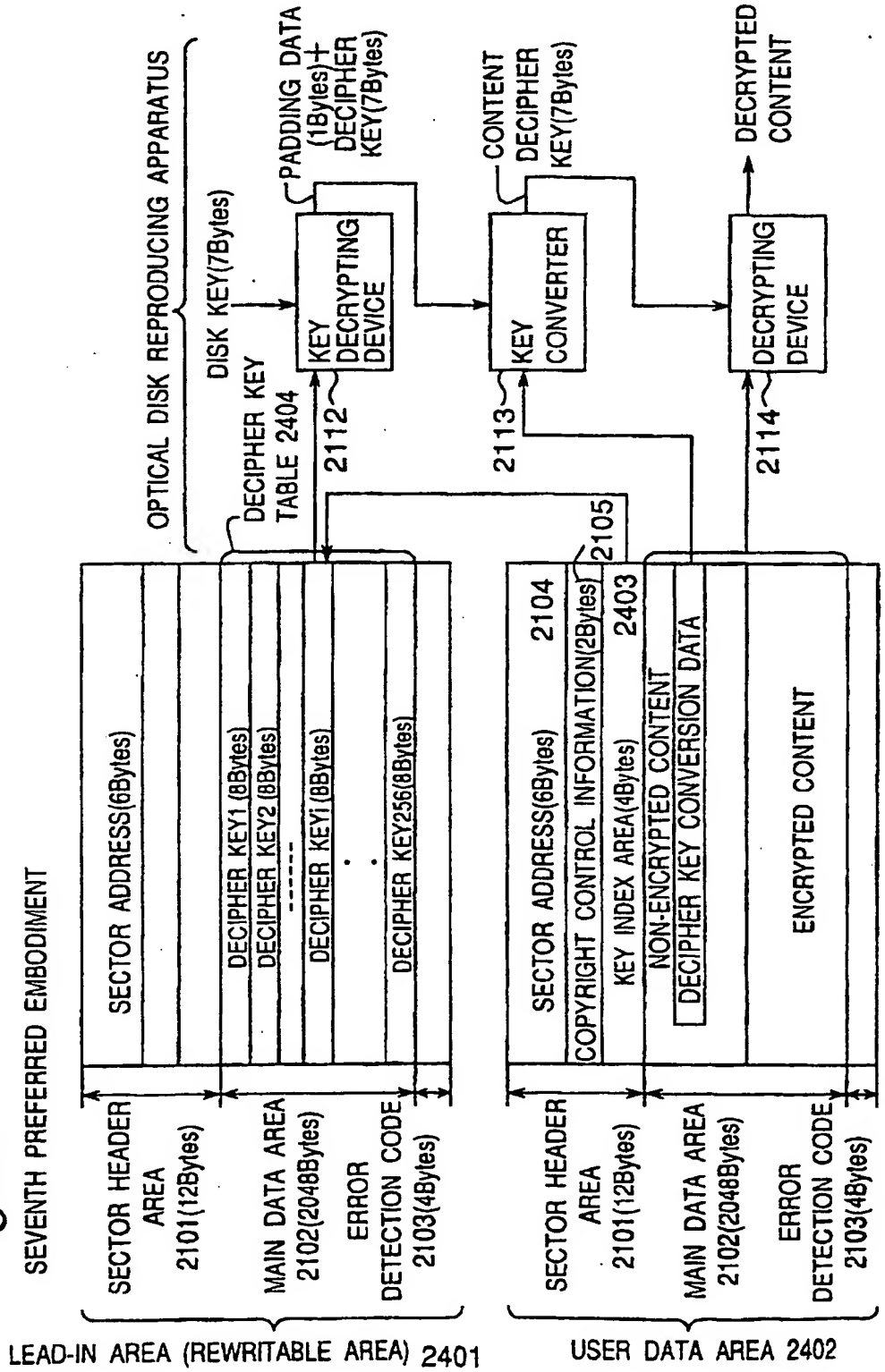


Fig.30A REPRESENTATION OF NON-RECORDED STATUS WITH INITIAL VALUE OF DECIPHER KEY

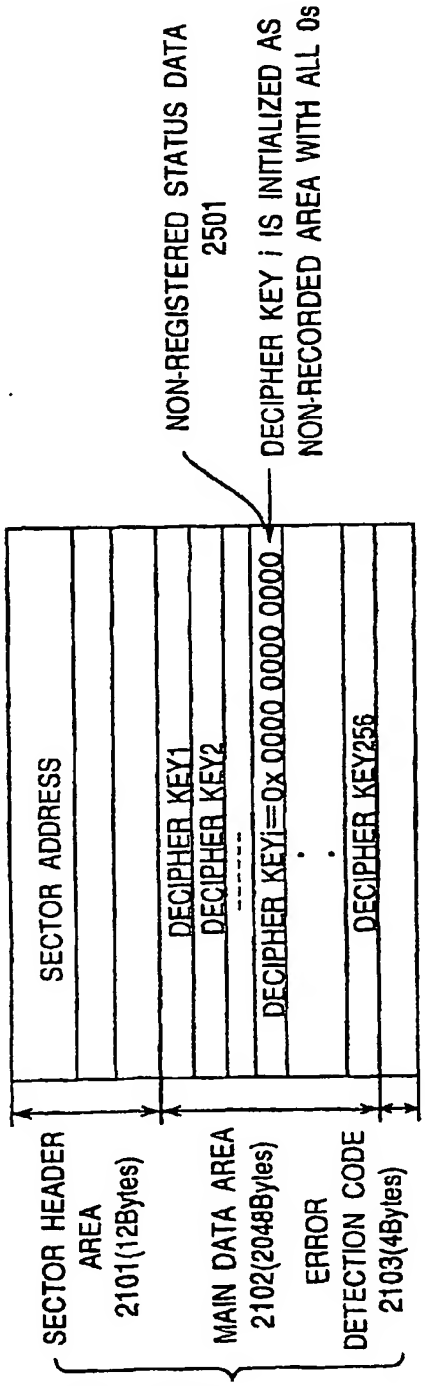



Fig.30B REPRESENTATION OF RECODED STATUS WITH DECIPHER KEY STATUS TABLE

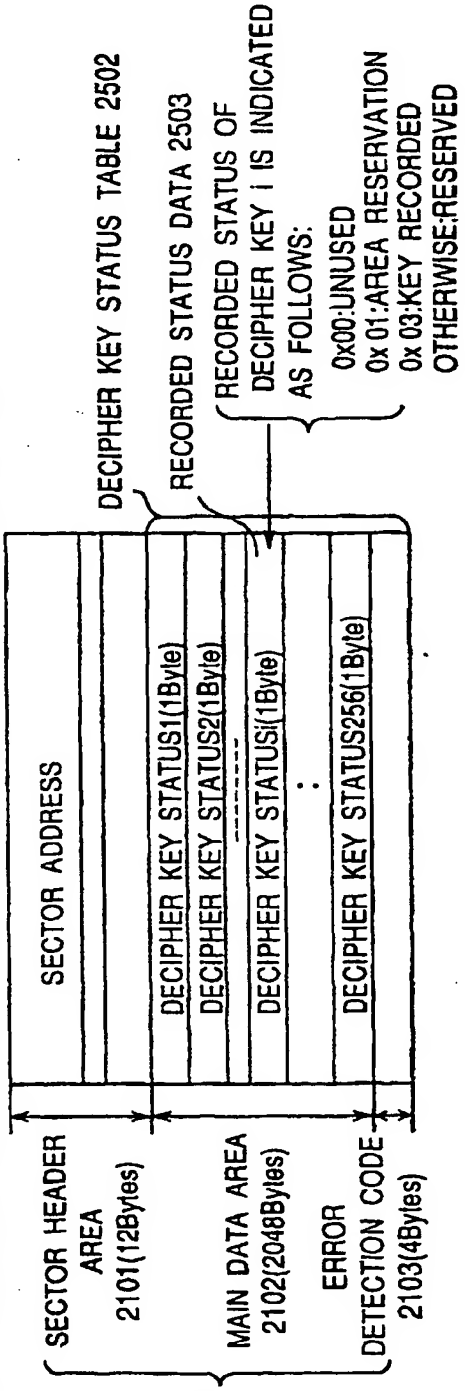


Fig.31

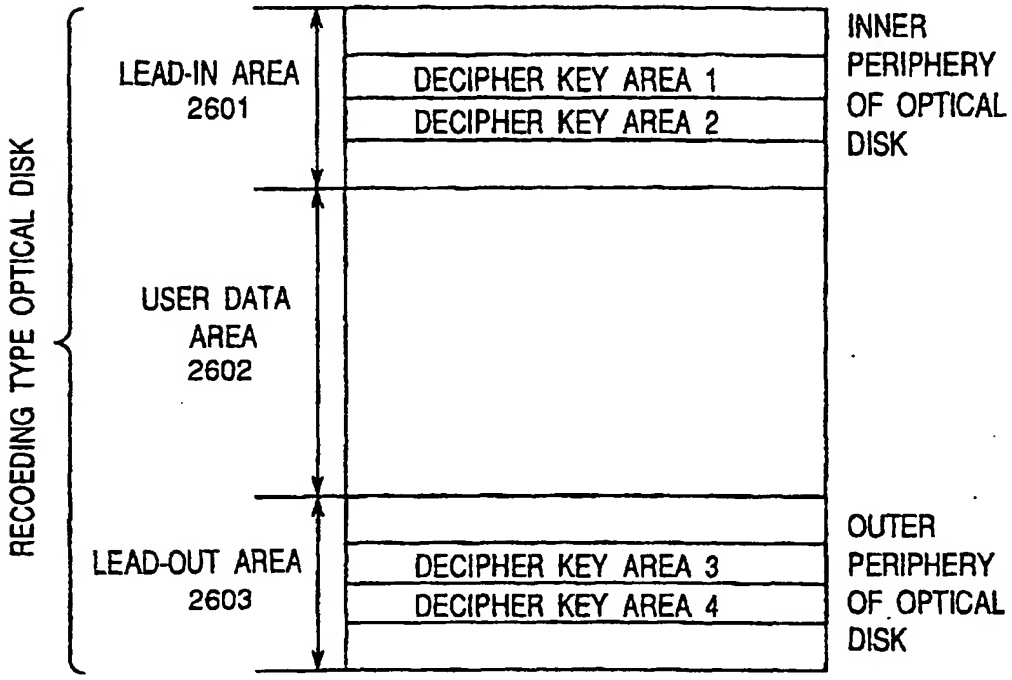

RECOEDING TYPE OPTICAL DISK
LEAD-IN AREA
2601
USER DATA
AREA
2602
LEAD-OUT AREA
2603
DECIPHER KEY AREA 1
DECIPHER KEY AREA 2
DECIPHER KEY AREA 3
DECIPHER KEY AREA 4
INNER
PERIPHERY
OF OPTICAL
DISK
OUTER
PERIPHERY
OF OPTICAL
DISK

Fig.32

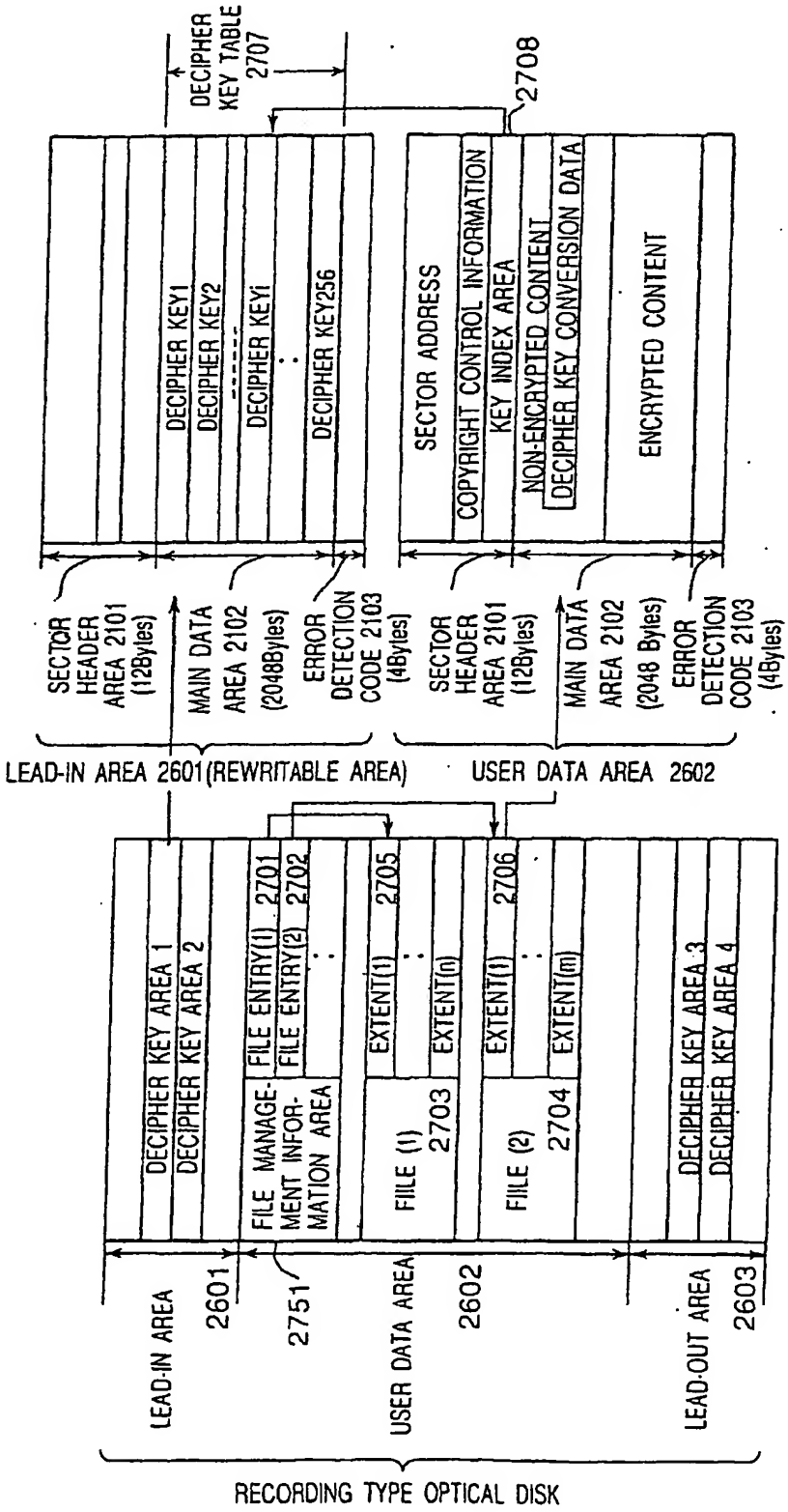

DECIPHER KEY TABLE 2707
2708
DECIPHER KEY1
DECIPHER KEY2
DECIPHER KEYi
DECIPHER KEY256
SECTOR ADDRESS
COPYRIGHT CONTROL INFORMATION
KEY INDEX AREA
NON-ENCRYPTED CONTENT
DECIPHER KEY CONVERSION DATA
ENCRYPTED CONTENT
SECTOR HEADER AREA 2101 (12Bytes)
MAIN DATA AREA 2102 (2048Bytes)
ERROR DETECTION CODE 2103 (4Bytes)
SECTOR HEADER AREA 2101 (12Bytes)
MAIN DATA AREA 2102 (2048 Bytes)
ERROR DETECTION CODE 2103 (4Bytes)
LEAD-IN AREA 2601(REWRITABLE AREA)
USER DATA AREA 2602
DECIPHER KEY AREA 1
DECIPHER KEY AREA 2
FILE ENTRY(1) 2701
FILE ENTRY(2) 2702
FILE MANAGE-MENT INFOR-MATION AREA
EXTENT(1) 2705
EXTENT(n)
FILE (1) 2703
EXTENT(1) 2706
EXTENT(m)
FILE (2) 2704
DECIPHER KEY AREA 3
DECIPHER KEY AREA 4
LEAD-IN AREA
2601
2751
USER DATA AREA
2602
LEAD-OUT AREA
2603
RECORDING TYPE OPTICAL DISK

*Fig.33*

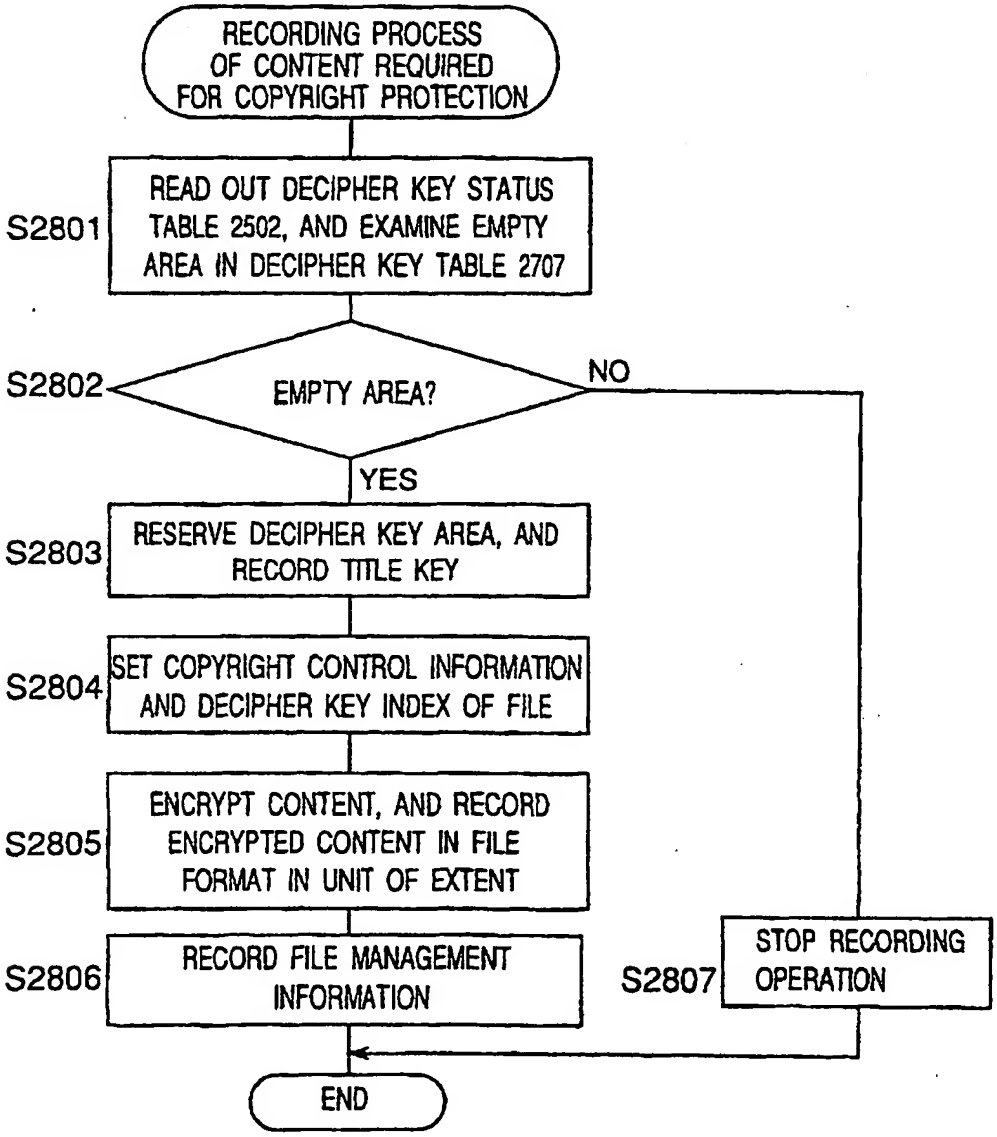

RECORDING PROCESS OF CONTENT REQUIRED FOR COPYRIGHT PROTECTION
S2801
READ OUT DECIPHER KEY STATUS TABLE 2502, AND EXAMINE EMPTY AREA IN DECIPHER KEY TABLE 2707
S2802
EMPTY AREA?
NO
YES
S2803
RESERVE DECIPHER KEY AREA, AND RECORD TITLE KEY
S2804
SET COPYRIGHT CONTROL INFORMATION AND DECIPHER KEY INDEX OF FILE
S2805
ENCRYPT CONTENT, AND RECORD ENCRYPTED CONTENT IN FILE FORMAT IN UNIT OF EXTENT
S2806
RECORD FILE MANAGEMENT INFORMATION
S2807
STOP RECORDING OPERATION
END

Fig.34

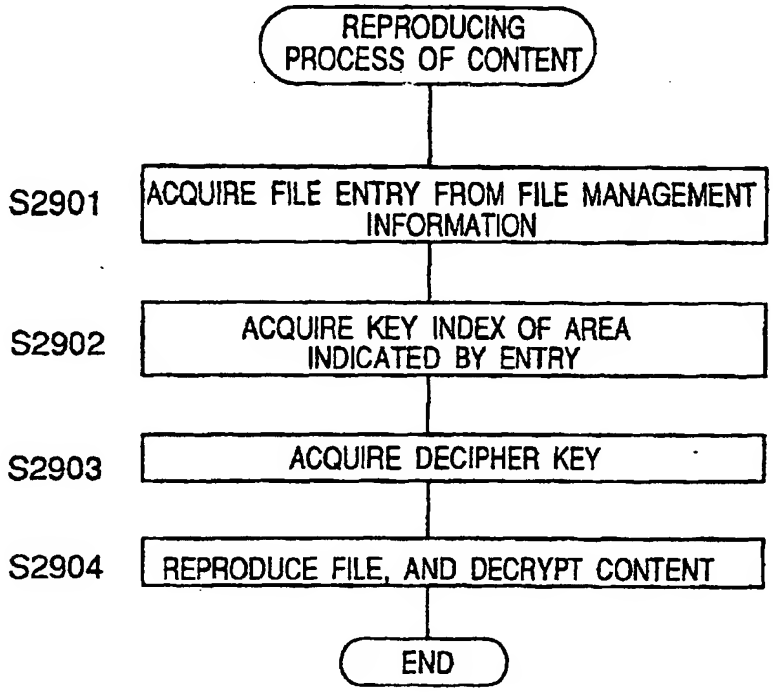
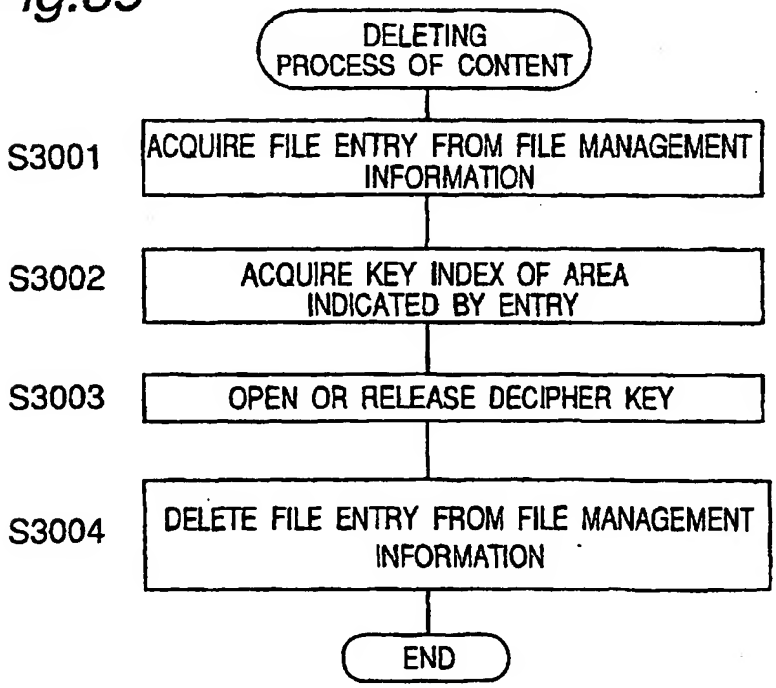

REPRODUCING PROCESS OF CONTENT
S2901
ACQUIRE FILE ENTRY FROM FILE MANAGEMENT INFORMATION
S2902
ACQUIRE KEY INDEX OF AREA INDICATED BY ENTRY
S2903
ACQUIRE DECIPHER KEY
S2904
REPRODUCE FILE, AND DECRYPT CONTENT
END

Fig.35


DELETING PROCESS OF CONTENT
S3001
ACQUIRE FILE ENTRY FROM FILE MANAGEMENT INFORMATION
S3002
ACQUIRE KEY INDEX OF AREA INDICATED BY ENTRY
S3003
OPEN OR RELEASE DECIPHER KEY
S3004
DELETE FILE ENTRY FROM FILE MANAGEMENT INFORMATION
END

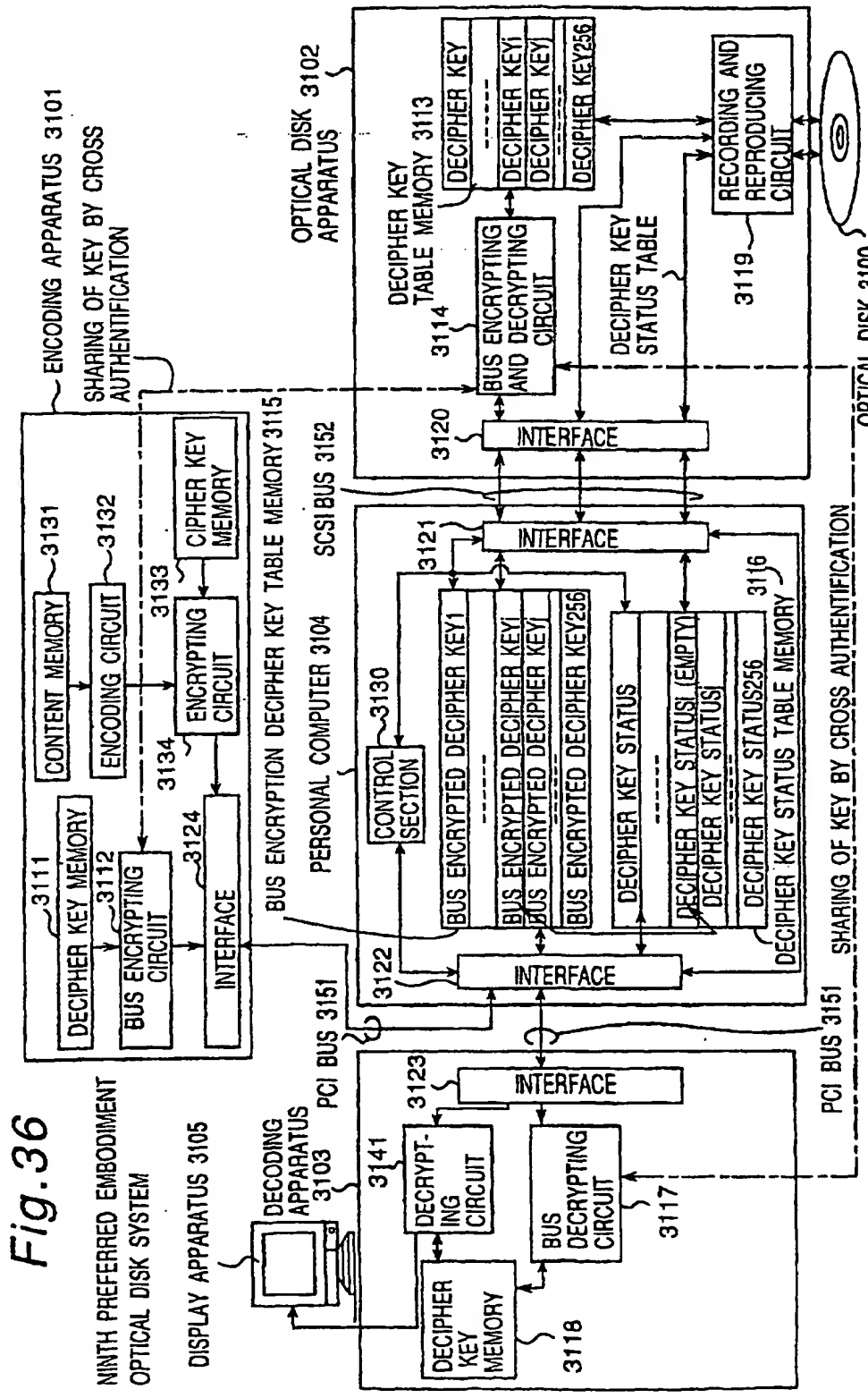

NINTH PREFERRED EMBODIMENT
OPTICAL DISK SYSTEM
DISPLAY APPARATUS 3105
DECODING APPARATUS 3103
PCI BUS 3151
DECRYPTING CIRCUIT 3141
BUS DECRYPTING CIRCUIT 3117
DECIPHER KEY MEMORY 3118
INTERFACE 3123
INTERFACE 3122
INTERFACE 3121
INTERFACE 3120
SCSI BUS 3152
PERSONAL COMPUTER 3104
CONTROL SECTION 3130
BUS ENCRYPTED DECIPHER KEY1
BUS ENCRYPTED DECIPHER KEYi
BUS ENCRYPTED DECIPHER KEY256
DECIPHER KEY STATUS
DECIPHER KEY STATUS1 (EMPTY)
DECIPHER KEY STATUSi
DECIPHER KEY STATUS256
DECIPHER KEY STATUS TABLE MEMORY 3116
BUS ENCRYPTION DECIPHER KEY TABLE MEMORY 3115
DECIPHER KEY TABLE MEMORY 3113
DECIPHER KEY
DECIPHER KEY1
DECIPHER KEYi
DECIPHER KEY256
BUS ENCRYPTING AND DECRYPTING CIRCUIT 3114
DECIPHER KEY STATUS TABLE
RECORDING AND REPRODUCING CIRCUIT 3119
OPTICAL DISK APPARATUS 3102
OPTICAL DISK 3100
SHARING OF KEY BY CROSS AUTHENTIFICATION
ENCODING APPARATUS 3101
SHARING OF KEY BY CROSS AUTHENTIFICATION
CONTENT MEMORY 3131
ENCODING CIRCUIT 3132
CIPHER KEY MEMORY 3133
ENCRYPTING CIRCUIT 3134
INTERFACE 3124
DECIPHER KEY MEMORY 3111
BUS ENCRYPTING CIRCUIT 3112

Fig.36

Fig.37

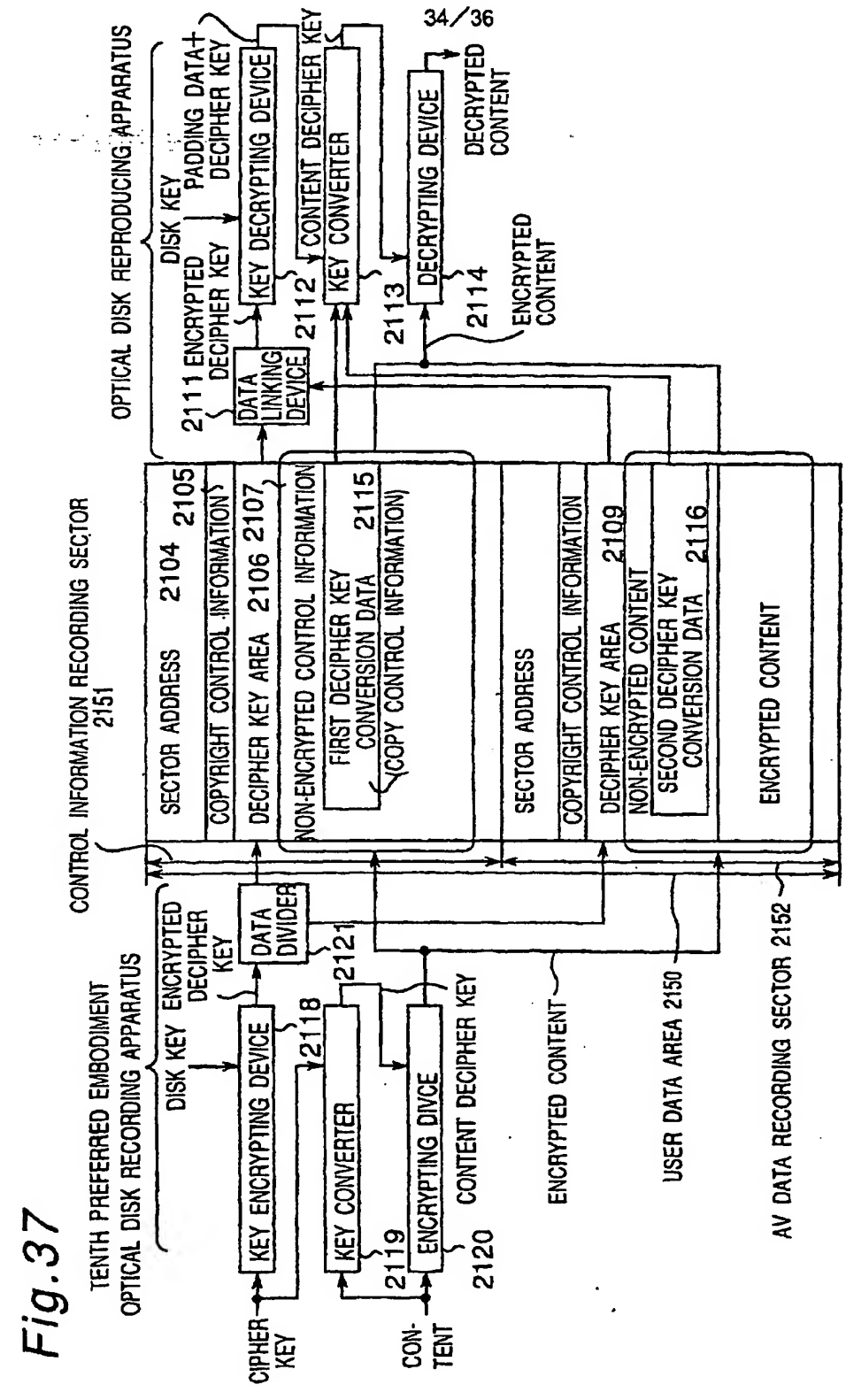

TENTH PREFERRED EMBODIMENT
OPTICAL DISK RECORDING APPARATUS
DISK KEY
ENCRYPTED DECIPHER KEY
KEY ENCRYPTING DEVICE
2118
KEY CONVERTER
2119
ENCRYPTING DIVCE
2120
CONTENT DECIPHER KEY
DATA DIVIDER
2121
CIPHER KEY
CON-TENT
CONTROL INFORMATION RECORDING SECTOR 2151
SECTOR ADDRESS 2104
2105
COPYRIGHT CONTROL INFORMATION
DECIPHER KEY AREA 2106
2107
NON-ENCRYPTED CONTROL INFORMATION
FIRST DECIPHER KEY CONVERSION DATA 2115
(COPY CONTROL INFORMATION)
SECTOR ADDRESS
COPYRIGHT CONTROL INFORMATION
DECIPHER KEY AREA 2109
NON-ENCRYPTED CONTENT
SECOND DECIPHER KEY CONVERSION DATA 2116
ENCRYPTED CONTENT
ENCRYPTED CONTENT
USER DATA AREA 2150
AV DATA RECORDING SECTOR 2152
OPTICAL DISK REPRODUCING APPARATUS
DISK KEY
PADDING DATA+ DECIPHER KEY
2111 ENCRYPTED DECIPHER KEY
DATA LINKING DEVICE
KEY DECRYPTING DEVICE
2112
CONTENT DECIPHER KEY
KEY CONVERTER
2113
DECRYPTING DEVICE
2114
ENCRYPTED CONTENT
34/36
DECRYPTED CONTENT

Fig.38

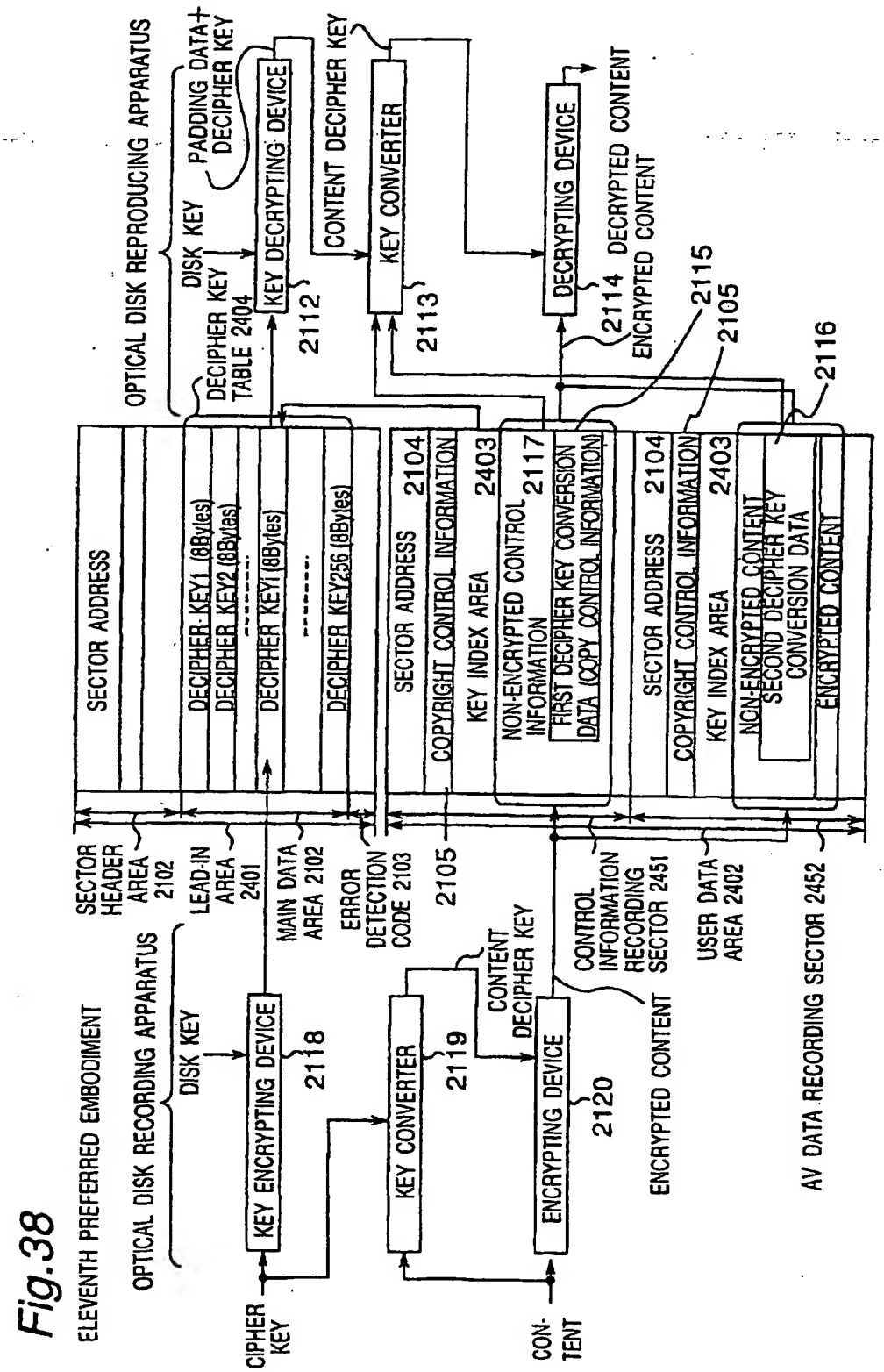

ELEVENTH PREFERRED EMBODIMENT
OPTICAL DISK RECORDING APPARATUS
DISK KEY
KEY ENCRYPTING DEVICE
2118
CIPHER KEY
KEY CONVERTER
2119
CONTENT DECIPHER KEY
ENCRYPTING DEVICE
2120
CON-TENT
SECTOR HEADER AREA 2102
LEAD-IN AREA 2401
MAIN DATA AREA 2102
ERROR DETECTION CODE 2103
2105
CONTROL INFORMATION RECORDING SECTOR 2451
ENCRYPTED CONTENT
USER DATA AREA 2402
AV DATA RECORDING SECTOR 2452
OPTICAL DISK REPRODUCING APPARATUS
DISK KEY
DECIPHER KEY TABLE 2404
PADDING DATA+ DECIPHER KEY
KEY DECRYPTING DEVICE
2112
CONTENT DECIPHER KEY
KEY CONVERTER
2113
DECRYPTING DEVICE
2114 DECRYPTED CONTENT
ENCRYPTED CONTENT
2115
2105
2116
SECTOR ADDRESS
DECIPHER KEY1 (8Bytes)
DECIPHER KEY2 (8Bytes)
DECIPHER KEY(8Bytes)
DECIPHER KEY256 (8Bytes)
SECTOR ADDRESS 2104
COPYRIGHT CONTROL INFORMATION
KEY INDEX AREA 2403
NON-ENCRYPTED CONTROL INFORMATION 2117
FIRST DECIPHER KEY CONVERSION DATA (COPY CONTROL INFORMATION)
SECTOR ADDRESS 2104
COPYRIGHT CONTROL INFORMATION
KEY INDEX AREA 2403
NON-ENCRYPTED CONTENT
SECOND DECIPHER KEY CONVERSION DATA
ENCRYPTED CONTENT

Fig.39 PRIOR ART